W64

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-239129
(43)Date of publication of application : 31.08.1999

(51)Int.CI. H04L 9/32
G06F 12/14
G06F 13/00
G09C 1/00
G09C 5/00
H04N 1/387

(21)Application number : 10-106438
(22)Date of filing : 16.04.1998

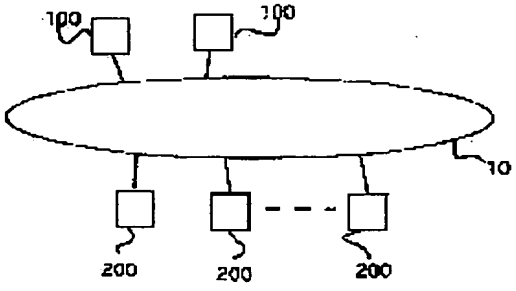
(71)Applicant : HITACHI LTD
(72)Inventor : YOSHIURA YUTAKA
SUZAKI SEIICHI
TAKARAGI KAZUO
SASAKI RYOICHI
TOYOSHIMA HISASHI
SAITO TSUKASA

(30)Priority

Priority number	Priority date	Priority country
09148061	05.06.1997	JP
09348860	18.12.1997	JP

(54) METHOD FOR CERTIFYING ELECTRONIC DATA

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a method for certifying electronic data by which the purchaser of the contents which become the original of an unauthorized copy can be specified with higher evidence.
SOLUTION: A provider device 100 sends the contents purchased by a purchaser to the device 200 of the purchaser after enciphering the contents by using the public key of the device 200 of the purchaser. The device 200 produces the electronic signature of the contents by using its own cryptographic key and buries the electronic signature in the sent contents in the form of an electronic watermark. Upon acquiring an unauthorized copy, the device 100 specifies the purchaser who has purchased the contents which become the original of the copy by verifying the electronic signature buried in the contents in the form of an electronic watermark.



LEGAL STATUS
[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

W64

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－239129

(43)公開日　平成11年(1999)８月31日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７５Ｂ
Ｇ０６Ｆ	12/14	３２０	Ｇ０６Ｆ	12/14	３２０Ｅ
	13/00	３５４		13/00	３５４Ｄ
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ	1/00	６４０Ｂ
	5/00			5/00	

審査請求　未請求　請求項の数19　ＯＬ　（全 32 頁）　最終頁に続く

(21)出願番号　特願平10－106438

(22)出願日　平成10年(1998)４月16日

(31)優先権主張番号　特願平9－148061
(32)優先日　平９(1997)６月５日
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願平9－348860
(32)優先日　平９(1997)12月18日
(33)優先権主張国　日本（ＪＰ）

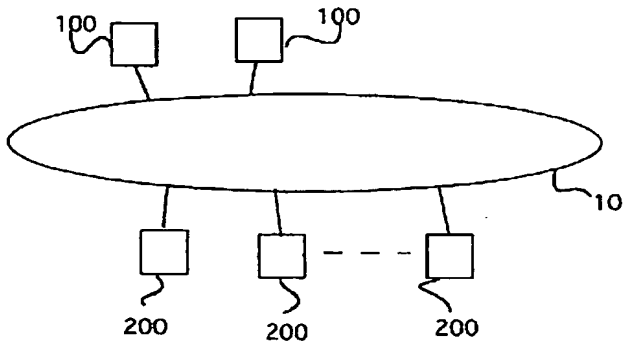
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　吉浦　裕
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　洲崎　誠一
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　宝木　和夫
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(74)代理人　弁理士　富田　和子

最終頁に続く

(54)【発明の名称】　電子データを認証するための方法

(57)【要約】
【課題】不正コピーの元となったコンテンツを購入した購入者を、より高い証拠性をもって特定する。
【解決手段】プロバイダー装置１００は、購入者装置２００の公開鍵を用いて、購入者が購入したコンテンツを暗号化して送付する。購入者装置２００は、自身の秘密鍵を用いてコンテンツの電子署名を作成し、作成した電子署名を電子透かしとして送付されたコンテンツに埋め込む。不正コピーを入手した場合、プロバイダー装置１００は、電子透かしの電子署名を検証し、この不正コピーの元となったコンテンツを購入した購入者を特定する。

図１



【特許請求の範囲】

【請求項１】電子計算機を用いて、コンテンツの埋め込み情報を処理するコンテンツ埋め込み情報の処理方法であって、

コンテンツの関係者の、公開鍵暗号体系に従った秘密鍵で、所定の情報を暗号化した暗号情報を作成するステップと、

作成した暗号情報を、コンテンツに、所定の規則に従って、少なくとも当該所定の規則を用いずに当該暗号情報のみを当該コンテンツから分離できないように埋め込むステップと、

を有することを特徴とするコンテンツ埋め込み情報の処理方法。

【請求項２】請求項１記載のコンテンツ埋め込み情報の処理方法であって、

暗号情報が埋め込まれたコンテンツから、暗号情報を抽出するステップと、

抽出した暗号情報を、コンテンツの関係者の公開鍵で復号化した結果が、前記所定の情報と一致するかを検証するステップと、

を有することを特徴とするコンテンツ埋め込み情報の処理方法。

【請求項３】請求項１記載のコンテンツ埋め込み情報の処理方法であって、

前記所定の情報を、前記暗号情報を埋め込むコンテンツの内容に依存した値をとる情報とすることにより、前記コンテンツの関係者の、当該コンテンツに対する電子署名を前記暗号情報としたことを特徴とするコンテンツ埋め込み情報の処理方法。

【請求項４】請求項１記載のコンテンツ埋め込み情報の処理方法であって、

前記暗号情報の作成に先立ち、コンテンツの内容をハッシュ関数で評価し、評価した評価値であるハッシュ値を前記所定の情報として生成するステップを設けることにより、前記コンテンツの関係者の、当該コンテンツに対する電子署名を前記暗号情報としたことを特徴とするコンテンツ埋め込み情報の処理方法。

【請求項５】電子計算機を用いて、コンテンツに、ｋ（ｋは２以上の整数）人のコンテンツ関係者の情報を埋め込むコンテンツ埋め込み情報の処理方法であって、

第１番目のコンテンツ関係者の、公開鍵暗号体系に従った秘密鍵で、コンテンツを第１のハッシュ関数で評価したｎビットのハッシュ値を、暗号化した電子署名を、コンテンツに、所定の規則に従って、少なくとも当該所定の規則を用いずに当該電子署名のみを当該コンテンツから分離できないように埋め込むステップと、

第２番目のコンテンツ関係者から第ｋ番目のコンテンツ関係者まで、順次、当該順番に従って、各コンテンツ関係者についての埋め込み処理を繰り返すステップとを有し、

第ｉ（ただし、ｉは２以上ｋ以下の整数）番目のコンテンツ関係者についての前記埋め込み処理は、第１番目から第（ｉ-1）番目までのコンテンツ関係者の電子署名が埋め込まれたコンテンツを第２のハッシュ関数で評価したｎ／２ビットのハッシュ値を、第ｉ番目のコンテンツ関係者の秘密鍵で暗号化した電子署名を、第１番目から第（ｉ-1）番目までのコンテンツ関係者の電子署名が埋め込まれたコンテンツに、所定の規則に従って、少なくとも当該所定の規則を用いずに当該電子署名のみを当該コンテンツから分離できないように埋め込む処理であることを特徴とするコンテンツ埋め込み情報の処理方法。

【請求項６】電子計算機を用いて、コンテンツに、ｋ（ｋは２以上の整数）人のコンテンツ関係者の情報を埋め込むコンテンツ埋め込み情報の処理方法であって、

第１番目のコンテンツ関係者の公開鍵暗号体系に従った秘密鍵で、コンテンツを第１のハッシュ関数で評価したハッシュ値を暗号化した、当該第１番目のコンテンツ関係者の電子署名を作成するステップと、

第２番目のコンテンツ関係者から第ｋ番目のコンテンツ関係者まで、順次、当該順番に従って、各コンテンツ関係者について、当該コンテンツ関係者の電子署名を作成する電子署名作成処理を繰り返すステップと、

第ｋ番目のコンテンツ作成者について実行された前記電子署名作成処理によって得られた第ｋ番目のコンテンツ作成者の電子署名をコンテンツに、所定の規則に従って、少なくとも当該所定の規則を用いずに当該電子署名のみを当該コンテンツから分離できないように埋め込むステップとを有し、

第ｉ（ただし、ｉは２以上ｋ以下の整数）番目のコンテンツ関係者についての前記電子署名作成処理は、第（ｉ-1）番目のコンテンツ関係者の電子署名の値に依存して定まる値を、第ｉ番目のコンテンツ関係者の秘密鍵で暗号化し、第ｉ-1番目のコンテンツ関係者の電子署名とする処理であることを特徴とするコンテンツ埋め込み情報の処理方法。

【請求項７】請求項６記載のコンテンツ埋め込み情報の処理方法であって、

前記第（ｉ-1）番目のコンテンツ関係者の電子署名の値に依存して定まる値は、前記第（ｉ-1）番目のコンテンツ関係者の電子署名の値を、ハッシュ関数で評価したハッシュ値であることを特徴とするコンテンツ埋め込み情報の処理方法。

【請求項８】情報開示者と情報閲覧者の双方が信頼する管理者によって管理されていて、かつ、真正性を確認可能なマルチメディアデータを、情報開示者は自己が公開する情報に対して付加し、情報閲覧者は該マルチメディアデータの真正性が確認されたかどうかに応じて前記情報の真正性を確認することを特徴とする情報の認証方法。

【請求項９】少なくとも１つのクライアント端末と、前

記クライアント端末からの要求に応じて情報提供を行う少なくとも１つのWWWサーバと、前記クライアント端末やWWWサーバで使用されるマークを管理する少なくとも１つのマーク管理サーバと、が通信網を介して相互に接続されているシステムにおいてWWWサーバが公開するＷｅｂページを認証する方法であって、
前記WWWサーバが、自WWWサーバのＵＲＬデータを含むマーク送付要求を前記マーク管理サーバに送るステップと、
前記WWWサーバが、前記マーク管理サーバから返送されてきたマークを自己のＷｅｂページに貼り付けた後、該マークに前記マーク管理サーバへのリンク情報を設定し、前記クライアント端末からアクセス可能な状態で該マーク付きＷｅｂページを公開するステップと、
前記マーク管理サーバが、自マーク管理サーバの管理対象であるマークの送付状況などをマーク管理ＤＢに記憶するステップと、
前記マーク管理サーバが、前記WWWサーバからのマーク送付要求を受け取った場合に、該WWWサーバがマークを取得する条件を満たしているかどうかを判定し、条件を満たしていると判定した場合にのみ、前記マーク管理ＤＢを更新してから、前記要求のあったマークを当該WWWサーバに返送するステップと、
前記マーク管理サーバが、前記クライアント端末からの真正性確認要求を受け取った場合に、前記マーク管理ＤＢを参照して該要求のあったマークの真正性を検証し、該検証結果を当該クライアント端末に返送するステップと、
前記クライアント端末が、前記WWWサーバから前記マーク付きＷｅｂページをダウンロードするステップと、
前記クライアント端末が、前記ダウンロードしたマーク付きＷｅｂページのＵＲＬデータを含む真正性確認要求をマーク管理サーバに送り、当該検証結果を受け取るステップとを備えていることを特徴とする方法。
【請求項１０】少なくとも１つのクライアント端末と、前記クライアント端末からの要求に応じて情報提供を行う少なくとも１つのWWWサーバと、前記クライアント端末やWWWサーバで使用されるマークを管理する少なくとも１つのマーク管理サーバと、が通信網を介して相互に接続されているシステムにおいてWWWサーバが公開するＷｅｂページを認証する方法であって、
前記WWWサーバが、自WWWサーバのＵＲＬデータを含むマーク送付要求を前記マーク管理サーバに送るステップと、
前記WWWサーバが、前記マーク管理サーバから返送されてきた署名付きマークを自己のＷｅｂページに貼り付た後、前記クライアント端末からアクセス可能な状態で該マーク付きＷｅｂページを公開するステップと、
前記マーク管理サーバが、自マーク管理サーバの管理対象であるマークの送付状況などをマーク管理ＤＢに記憶するステップと、
前記マーク管理サーバが、前記クライアント端末からの公開鍵送付要求を受け取った場合に、自マーク管理サーバの公開鍵を当該クライアント端末に返送するステップと、
前記マーク管理サーバが、前記WWWサーバからのマーク送付要求を受け取った場合に、該WWWサーバがマークを取得する条件を満たしているかどうかを判定し、条件を満たしていると判定した場合にのみ、前記マーク管理ＤＢを更新してから、前記要求に含まれる前記WWWサーバのＵＲＬデータに電子的な署名を施し、要求のあったマークと該署名とを一纏めにして署名付きマークを生成して当該WWWサーバに返送するステップと、
前記クライアント端末が、公開鍵送付要求を前記マーク管理サーバに送るステップと、
前記クライアント端末が、前記マーク管理サーバから返送されてきた該マーク管理サーバ公開鍵を、公開鍵ＤＢに記憶するステップと、
前記クライアント端末が、前記WWWサーバから前記マーク付きＷｅｂページをダウンロードするステップと、
前記クライアント端末が、前記公開鍵ＤＢを参照して、前記ダウンロードしたマーク付きＷｅｂページに含まれる署名を検証するステップとを有することを特徴とする方法。
【請求項１１】請求項１０記載の方法であって、
署名付きマークを生成する場合に、前記WWWサーバのＵＲＬデータに加えて、マークとして用いている画像データも署名対象とし、該マークと署名とから署名付きマークを生成することを特徴とする方法。
【請求項１２】請求項１０記載の方法であって、
署名付きマークを生成する場合に、さらに、前記Ｗｅｂページも署名対象とし、該マークと署名とから署名付きマークを生成することを特徴とする方法。
【請求項１３】請求項１０記載の方法であって、
署名付きマークを生成する場合に、マークと署名とだけでなく、本システムに関連した何らかの属性情報も署名付きマークの構成要素の一つとすることを特徴とすることを特徴とする方法。
【請求項１４】電子計算機を用いて、電子データに当該電子データを認証するための認証用データを含めた認証可能電子データを作成する方法であって、
電子データの利用時に利用者が認知可能な出力を行うマーク用データを生成するステップと、
前記マーク用データに所定の情報を電子透かしとして埋め込んだ、透かし入りマーク用データを生成するステップと、
生成した透かし入りマーク用データを、前記電子データに含め、前記認証可能電子データを生成するステップとを有することを特徴とする方法。
【請求項１５】請求項１４記載の方法であって、

前記所定の情報は、前記電子データを所定のハッシュ関数で評価したハッシュ値であることを特徴とする方法。
【請求項１６】請求項１４記載の方法であって、
前記所定の情報は、前記電子データを所定の関数で評価した評価値を、所定の公開鍵暗号法に従った秘密鍵で暗号化した電子署名であることを特徴とする方法。
【請求項１７】請求項１４記載の方法であって、
前記認証可能電子データから前記マーク用データを切り出すステップと、
切り出した前記マーク用データから電子透かしとして埋め込まれた前記所定の情報を抽出するステップと、
抽出した情報に基づいて電子データを認証するステップとを有することを特徴とする方法。
【請求項１８】請求項１５記載の方法であって、
前記認証可能電子データから前記マーク用データを切り出すステップと、
切り出した前記マーク用データから電子透かしとして埋め込まれたハッシュ値を抽出するステップと、
前記認証可能電子データに基づいて、前記電子データを前記所定のハッシュ関数で評価したハッシュ値を算出するステップと、
抽出したハッシュ値と算出したハッシュ値が一致した場合に、電子データの認証が成功したと判定するステップとを有することを特徴とする方法。
【請求項１９】請求項１６記載の方法であって、
前記認証可能電子データから前記マーク用データを切り出すステップと、
切り出した前記マーク用データから電子透かしとして埋め込まれた電子署名を抽出するステップと、
抽出した電子署名を前記秘密鍵に対応する公開鍵で復号化して得られる評価値を抽出する手段と、
前記認証可能電子データに基づいて、前記電子データを前記所定の関数で評価した評価値を算出するステップと、
抽出したハッシュ値と算出したハッシュ値が一致した場合に、電子データの認証が成功したと判定するステップとを有することを特徴とする方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、電子データと個人／機関との関係を認証可能とする技術に関するものである。
【０００２】
【従来の技術】近年の情報化社会の発展に伴い、電子データが、従来の伝統的な印刷物に代わって、各種情報の伝達媒体として利用されることが増えている。また、電子データ自身が、価値ある商品として商取引の対象となることもある。
【０００３】このような情報化社会では、電子データの不正な複製や改竄や使用による犯罪や、悪意ある行為を防ぐために、電子データと個人／機関との関係を認証可能とすることが必要となる。たとえば、電子データが何かしらの権限ある機関により保証されたものであるかどうかを確認できるようにするためには、その電子データと権限ある機関との関係が認証可能である必要がある。同様に、電子データの出所や電子データに対して保有する個人や機関の権利などを確認するためには、その電子データと個人や機関との関係が認証可能である必要がある。
【０００４】従来、電子データと個人／機関との関係を認証可能とする技術としては、電子署名と呼ばれる技術が知られている。
【０００５】電子署名は、暗号理論入門、共立出版（1993年）133頁～１３７頁などに記載されているように、書類の真正さを保証するための技術であり、公開鍵暗号技術と一方向性関数を組み合わせたものである。
【０００６】この技術では、まず、ｇ（ｆ（ｎ，Ｓ），Ｖ）＝ｎ、ｆ（ｇ（ｎ，Ｖ），Ｓ）＝ｎが成立する秘密鍵Ｓ、公開鍵Ｖの組を作成する。ここでｎは任意のデータ、ｆ、ｇは所定の関数であり、上記式は、秘密鍵Ｓを用いて暗号化した任意のデータは公開鍵Vを用いて復号化することができ、また、逆に、公開鍵Vを用いて暗号化した任意のデータは秘密鍵Sで復号化できることを表している。また、ここで、公開鍵Ｖから秘密鍵Ｓを求めることは実質的に不可能となっている。
【０００７】秘密鍵Ｓ、公開鍵Ｖを作成したならば、作成者は公開鍵Ｖを、相手方に渡し、秘密鍵Ｓは作成者が秘密に保持する。
【０００８】そして、鍵の作成者が、相手方にデータを送る場合には、データを所定の一方向関数で評価した評価値を秘密鍵Sで暗号化した電子署名をデータに添付して相手方に渡す。
【０００９】ここで、一方向関数は、実質上、データから関数で評価した評価値を算出可能であるが、評価値から元のデータを算出することは実質的に実用上不可能である性質をもつ。また、この電子署名で用いる一方向関数には、実質的に異なるデータに対して異なるビット列を返す関数であること、すなわち、異なるデータに対して同じビット列を返す確率が極めて低い関数であること必要となる。このような関数としては、データの評価値として所定のビット列を返す一方向ハッシュ関数などが知られている。ここで一方向ハッシュ関数を、hで表した場合の、データＤの一方向ハッシュ関数による評価値ｈ（Ｄ）をＤのハッシュ値と呼ぶ。
【００１０】さて、電子署名が添付されたデータを受け取った相手方は、データを一方向関数で評価して評価値を求め、この評価値が、電子署名を公開鍵Ｖを用いて復号化した値と一致するかを検証する。そして、一致した場合には、電子署名が公開鍵Ｖに対応する秘密鍵Sの保持者によって成されたものであり、かつ、その電子署名

の対象が受け取ったデータであることを認証する。

【００１１】また、一つのデータに対して複数人の電子署名を行う技術として、Applied Cryptography, Jhon Wilsy & SOns, Inc. (1996), pp 39-41に記載の技術が知られている。

【００１２】この技術は、各自がデータのハッシュ値を電子署名として用いるのでなく、第２番目以降の署名者は、前の署名者の電子署名のハッシュ値を自身の電子署名として用いるものである。すなわち、第１番目の署名者は、上述したのと同様にデータのハッシュ値を自身の秘密鍵で暗号化し電子署名とする。そして、第２番目の署名者は第１番目の署名者の電子署名のハッシュ値を自身の秘密鍵で暗号化し自身の電子署名とする。以降、同様に、第ｎ番目の署名者は、前の署名者の電子署名のハッシュ値を、第ｎ番目の秘密鍵で暗号化して、第ｎ番目の署名者の電子署名とする。

【００１３】この場合、ｎ人の署名者によって成された電子署名の検証は、次のように行う。すなわち、電子署名を、第ｎ番目の署名者の公開鍵で復号化し、復号した電子署名を第n-1番目の署名者の公開鍵で復号化するといったように、順次、復号化し、第１番目の公開鍵で復号化した結果が、データのハッシュ値と一致すれば、この電子署名は、各公開鍵の所有者であるｎ人の署名者によって、当該データに対して成されたものであるとする。ただし、署名者の署名の順序が分からない場合などには、全ての署名者の順列について検証する必要が生じる。

【００１４】また、従来、電子データを、個人／機関との関係において認証可能とする技術としては、電子透かし（digital watermark）と呼ばれる技術が知られている。

【００１５】この技術は、日経エレクトロニクス（1997年）６８３号９９頁から107頁などに記載されているように、イメージデータの著作権などの管理情報を、イメージデータ自体にイメージデータと不可分に埋め込む技術である。

【００１６】この電子透かしの技術は、次のような特徴を持っている。すなわち、埋め込まれた情報は、情報を埋め込んだイメージデータを表示した場合にも一般的には視認されず、また、視認可能な範囲において画像自体をほとんど変化させない。一方、埋め込まれた情報のみを正確に除去することは容易でない反面、不正確に除去すると画像の画質が著しく劣化する。また、一般的には、ある程度までは、イメージデータを圧縮した場合にも、埋め込んだ情報を復元することができる。

【００１７】この他、電子透かしの技術としては、イメージデータを対象とするのではなく、テキストやドロウデータ（図面データ）やオウディオデータを対象とするものなどが提案されている。

【００１８】なお、日経エレクトロニクス（1997年）６８３号９９頁から107頁には、このような電子透かしを利用して、イメージデータなどの電子データであるコンテンツの不正コピーを防止する技術も記載されている。

【００１９】この技術は、コンテンツに、コンテンツを購入した者の識別情報を電子透かしとして埋め込み、不正コピーされたコンテンツが押収されたときには、これに埋め込まれた情報を抽出し、不正コピーを行った者（すなわち購入者）を特定するものである。

【００２０】ここで、このような購入者の識別情報のコンテンツへの埋込みは、基本的には以下の手順で行われる。

【００２１】（１）購入者がコンテンツの購入を希望したら、プロバイダー（コンテンツの提供者）はその購入者にユニークな番号を割り当てる。

【００２２】（２）プロバイダーは、コンテンツに、そのコンテンツの購入者の番号を電子透かしとして埋め込む。

【００２３】（３）不正コピーされたコンテンツをプロバイダーまたは監査機関が押収したときに、そのコンテンツから購入者の番号を抽出し、購入者を特定する。

【００２４】（４）購入者がコンテンツの不正コピーを行った、あるいは、不正コピー者にコンテンツを手渡したとして、購入者にペナルティを科す。

【００２５】ところで、近年の、インターネットのようなオープンなネットワークを使って、複数のユーザに情報を開示・伝達する手段として、Ｗｏｒｌｄ Ｗｉｄｅ Ｗｅｂ（WWW）サーバプログラムとブラウザプログラムとを用いるWWWシステムの普及や利用範囲の拡大に伴い、WWWサーバ上で公開される電子データであるwebページについても、WWWシステムの不正な使用による犯罪や、悪意ある行為を防ぐために、webページを、個人／機関との関係において認証可能とすることが必要となる。たとえば、webページ上で何かしらの権限ある機関により保証されたものであることが提示されている場合に、真に、そのwebページが権限ある機関により保証されたものであることを確認できるようにするためには、そのwebページが権限ある機関との関係において認証可能である必要がある。同様に、webページの発信者やwebページに対して保有する個人や機関の権利などを確認するためには、そのwebページが個人や機関との関係において認証可能である必要がある。

【００２６】なお、たとえば「ＯＰＥＮ ＤＥＳＩＧＮ ９６年４月号」（発行人：蒲生良治、発行所：ＣＱ出版株式会社）の４ページから２２ページおよび４０ページから７８ページに記載されているように、WWWシステムは、操作性に優れたグラフィカルユーザインタフェース（ＧＵＩ）を備えているとともに、関連性のある様々な情報をハイパーリンクでつなぐことで簡単に参照できるようにすることができるなどユーザの利便性にも優れており、今日のこれほどまで急速なインターネットの

発展は、このWWWシステムによるところが大である。

【００２７】この文献に記載されたWWWシステムの概要を簡単に説明する。

【００２８】WWWシステムは、情報を公開するためのWWWサーバプログラムが動作する少なくとも一つのWWWサーバと、当該公開情報を閲覧するためのブラウザプログラムが動作する少なくとも一つのクライアント端末からなり、WWWサーバとクライアント端末との間は、ＨＴＴＰ（ＨｙｐｅｒＴｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）と呼ばれる通信プロトコルによりデータのやり取りが行われる。

【００２９】WWWサーバで情報を公開する場合、まず、当該サーバに格納された公開すべきテキストデータ、イメージデータ、オウディオデータ、ビデオデータ、あるいは他Ｗｅｂページへのハイパーリンクデータなどを、ＨＴＭＬ（Ｈｙｐｅｒ　Ｔｅｘｔ　Ｍａｋｅｕｐ　Ｌａｎｇｕａｇｅ）と呼ばれる構造記述言語を用いて相互に関連付けて一纏めにしたＷｅｂページを作成する。次に、このＷｅｂページを、他のコンピュータ（クライアント端末や他のWWWサーバ）からアクセス可能な状態で、WWWサーバの任意の格納場所（ディレクトリ）に保管する。

【００３０】一方、公開されたＷｅｂページを、ユーザがクライアント端末からブラウザプログラムを用いて閲覧する場合、クライアント端末を利用するユーザがブラウザプログラムに対して、上記ＷｅｂページのＵＲＬ（Ｕｎｉｖｅｒｓａｌ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）を指定すると、そのＷｅｂページのデータがWWWサーバよりクライアント端末に送られる。そして、そのＷｅｂページに含まれるテキストデータ、イメージデータ、ビデオデータなどがクライアント端末の画面上に表示される。また、オウディオデータは当該クライアント端末に接続されたスピーカーなどから出力される。

【００３１】ところで、近年では、このようなWWWシステムを単なる情報伝達手段としてだけでなく、ビジネスに利用しようという動きが顕著である。たとえば、WWWシステムにより商品情報を公開するいわゆる電子商取引システムなどはそのようなビジネス利用の代表例である。

【００３２】このような電子商取引システムの概要については、たとえば「情報処理　第３８巻　第９号」（発行人：飯塚　浩司、発行所：社団法人　情報処理学会）の７５２ページから８１０ページに記載されている。

【００３３】この文献では、上記電子商取引システムを、単なる商品情報を消費者に開示するためだけのシステムではなく、共通鍵暗号や公開鍵暗号といった暗号技術や、ディジタル署名などの認証技術を駆使し、決済までも行うシステムとして提示している。また、この場合における決済方法としては銀行決済やクレジット決済、あるいは電子マネーによる決済などいろいろな方法を取ることを想定している。

【００３４】このような電子商取引システムでは、販売者は、自己のＷｅｂページに利用可能なクレジットカード会社のロゴマークなどのイメージデータを含め、消費者が支払方法を一目で認識できるようにすることが多い。これは、現実世界（インターネットのようなバーチャルな世界ではない）において、各販売店（クレジットカード会社の加盟店）に、そこで使用可能なクレジットカードのロゴマークが掲示されているのと同様である。

【００３５】また、この他、Ｗｅｂページの発信者を示すロゴマークや、そのwebページを承認した何らかの権限ある個人／機関を示すロゴマークなどのイメージデータをＷｅｂページに含め、webページの利用者が、一目で、webページの発信者やwebページが権限ある個人／機関に承認されていることを認識できるようにすることもある。

【００３６】

【発明が解決しようとする課題】前記、電子透かしの技術によれば、次のような問題がある。

【００３７】まず、第１に、電子透かしとして埋め込まれた情報と、当該情報が提示する個人／機関との関係が保証されない。すなわち、電子データに埋め込まれた情報が、個人／機関と電子データ関係を正しく表していることを保証できない。

【００３８】このため、たとえば、前述した不正コピーを防止する技術では、不正コピーコンテンツに埋め込まれた番号が、真に不正コピーされたコンテンツを購入した者を示す番号であるという証拠となりにくい。すなわち、プロバイダーが購入者に一方的に与える番号であるため、購入者は、番号と自身との対応を否認できる可能性がある。

【００３９】また、前述したwebページの場合は、不正者が、他人を示す情報を偽造して電子透かしとして埋め込んで、他人を装ったり、権限ある機関に保証されていることを装う可能性を否定できない。

【００４０】第２に、電子データと、電子透かしとして埋め込まれた情報が示す個人／機関との関係が保証されない。

【００４１】このため、たとえば、前述した不正コピーを防止する技術では、購入者の番号が、購入者が買ったコンテンツに正しく埋め込まれたという証拠がない。すなわち、購入者が買っていないコンテンツに、購入者以外（例えばプロバイダーの内部者）が誤って、もしくは、不正目的で購入者番号を埋め込んだ可能性を否定できない。

【００４２】また、前述したwebページの場合は、個人／機関が正規のwebページに対して埋め込んだ電子透かしを抽出し、不正目的で作成したwebページに対して電子透かしとして埋め込んで、他人を装ったり、権限ある機関に保証されていることを装う可能性を否定できな

い。

【００４３】また、第３に、電子透かしの技術によって、コンテンツに著作権の情報を埋め込む技術によれば、一つのコンテンツに対して多数の権利者が存在した場合、埋め込むべき情報量が多くなりコンテンツの質（例えば、コンテンツが画像である場合は画質）を大きく劣化させてしまう。また、第４に、電子透かしの技術は、webページのような複数種のデータを含む電子データに適していない。たとえば、テキスト、ドロウデータ（図面データ）、イメージデータを含む電子データに適用するためには、データの種類毎に異なった処理を行わなければならない。

【００４４】一方、前記電子署名の技術によれば、電子データに他に、電子署名を電子データと組で管理しなければならないという煩わしさがある。また、電子署名は、電子透かしに比べ電子データと分離することが極めて容易であるため、前述した不正コピーの防止の目的のために用いることができない。

【００４５】また、前記電子透かし、電子署名の技術とも、不可視であるため、電子透かし、電子署名が示す電子データと個人／機関との関係を、電子データの利用者に直接提示することができないという問題もある。

【００４６】たとえば、電子透かし、電子署名では、前述したロゴマークをイメージデータとして含めたwebページのように、一目でwebページと個人／機関との関係を利用者に提示することができない。また、このことは、電子透かし、電子署名が示す電子データと個人／機関との関係と、電子データが利用者に直接示す電子データと個人／機関との関係が一致していることが電子透かし、電子署名によっては直接保証されないことを意味する。

【００４７】一方、Ｗｅｂページ上にロゴマークをイメージデータとして含める技術によれば、ロゴマークが単なるイメージデータであるため、ロゴマークが示す個人／機関との関係をＷｅｂページが真に有しているのかどうかを認証することができない。

【００４８】このため、たとえば、前記クレジット会社のロゴマークを例にとれば、不正者が、当該クレジットカード会社の正規加盟店のＷｅｂページから当該ロゴマークをコピーし、自己の販売店のＷｅｂページの適当な個所に該ロゴマークを貼り付けてから、該Ｗｅｂページを他のコンピュータからアクセス可能な状態で、WWWサーバの任意の格納場所に保管した場合、消費者は、不正者のＷｅｂページに含まれる上記クレジットカード会社のロゴマークを見て、その不正者が正規の加盟店であるものと判断し、自己のクレジットカード番号など決済に必要なデータを当該WWWサーバに送信してしまう可能性がある。結果、不正者は、入手した消費者のクレジット番号を不正に入手し不正な利益を得ることが可能となる。

【００４９】そこで、本発明は、電子データと個人／機関との関係を、より高い信頼性をもって認証可能とする技術を提供することを課題とする。また、電子データとの関係を認証可能な個人／機関と一致することが保証されるように、電子データと関係を持つ個人／機関を電子データによって利用者に直接提示ことを課題とする。

【００５０】

【課題を解決するための手段】前記課題達成のために、本発明は、たとえば、電子計算機を用いて、コンテンツの埋め込み情報を処理するコンテンツ埋め込み情報の処理方法であって、コンテンツの関係者の、公開鍵暗号体系に従った秘密鍵で、所定の情報を暗号化した暗号情報を作成するステップと、作成した暗号情報を、コンテンツに、所定の規則に従って、少なくとも当該所定の規則を用いずに当該暗号情報のみを当該コンテンツから分離できないように埋め込むステップとを有することを特徴とするコンテンツ埋め込み情報の処理方法を提供する。

【００５１】ただし、ここで、少なくとも所定の規則を用いずに当該暗号情報のみを当該コンテンツから分離できないとは、所定の規則を用いない場合には、試行錯誤的な処理以外の処理で分離することができないことを意味する。

【００５２】このような方法によれば、暗号情報が埋め込まれたコンテンツから、暗号情報を抽出し、抽出した暗号情報を、コンテンツの関係者の公開鍵で復号化した結果が、前記所定の情報と一致するかを検証することにより、暗号情報が埋め込まれたコンテンツが不正コピーである場合に、当該不正コピーの元となったコンテンツの関係者を特定することができる。

【００５３】そして、この場合において、このような判断は、不正コピーに埋め込まれた、個々のコンテンツ関係者自身しか知らないことが保証されるコンテンツ関係者の秘密鍵に依存し、したがって購入者自身しか作成することのできない情報の検証によって行われるので、不正コピーに埋め込まれた情報と、不正コピーの起因となったコンテンツ関係者との対応の証拠性を向上することができる。

【００５４】また、埋め込む暗号情報を、暗号情報を埋め込むコンテンツの内容に依存した値をとる、たとえば、コンテンツのハッシュ値を秘密鍵で暗号化した電子署名とすれば、不正コピーに埋め込まれた情報が示すコンテンツ関係者のとコンテンツとの対応性の証拠性も向上することができる。

【００５５】また、本発明は、前記課題達成のために、電子計算機を用いて、コンテンツに、ｋ（ｋは２以上の整数）人のコンテンツ関係者の情報を埋め込むコンテンツ埋め込み情報の処理方法であって、第１番目のコンテンツ関係者の、公開鍵暗号体系に従った秘密鍵で、コンテンツを第１のハッシュ関数で評価したｎビットのハッシュ値を、暗号化した電子署名を、コンテンツに、所定

の規則に従って、少なくとも当該所定の規則を用いずに当該電子署名のみを当該コンテンツから分離できないように埋め込むステップと、第２番目のコンテンツ関係者から第ｋ番目のコンテンツ関係者まで、順次、当該順番に従って、各コンテンツ関係者についての埋め込み処理を繰り返すステップとを有し、第ｉ（ただし、ｉは２以上ｋ以下の整数）番目のコンテンツ関係者についての前記埋め込み処理は、第１番目から第（ｉ-１）番目までのコンテンツ関係者の電子署名が埋め込まれたコンテンツを第２のハッシュ関数で評価したｎ／２ビットのハッシュ値を、第ｉ番目のコンテンツ関係者の秘密鍵で暗号化した電子署名を、第１番目から第（ｉ-１）番目までのコンテンツ関係者の電子署名が埋め込まれたコンテンツに、所定の規則に従って、少なくとも当該所定の規則を用いずに当該電子署名のみを当該コンテンツから分離できないように埋め込む処理であることを特徴とするコンテンツ埋め込み情報の処理方法を提供する。

【００５６】この方法によれば、ｋ人の電子署名のコンテンツの埋め込みを、ｎ＋（ｋ-１）×ｎ／２ビットのデータの埋め込みで達成できる。また、後述するように、そのセキュリティを大きく劣化することもない。

【００５７】また、本発明が提供する電子計算機を用いて、コンテンツに、ｋ（ｋは２以上の整数）人のコンテンツ関係者の情報を埋め込むコンテンツ埋め込み情報の処理方法であって、第１番目のコンテンツ関係者の公開鍵暗号体系に従った秘密鍵で、コンテンツを第１のハッシュ関数で評価したハッシュ値を暗号化した、当該第１番目のコンテンツ関係者の電子署名を作成するステップと、第２番目のコンテンツ関係者から第ｋ番目のコンテンツ関係者まで、順次、当該順番に従って、各コンテンツ関係者について、当該コンテンツ関係者の電子署名を作成する電子署名作成処理を繰り返すステップと、第ｋ番目のコンテンツ作成者について実行された前記電子署名作成処理によって得られた第ｋ番目のコンテンツ作成者の電子署名をコンテンツに、所定の規則に従って、少なくとも当該所定の規則を用いずに当該電子署名のみを当該コンテンツから分離できないように埋め込むステップとを有し、第ｉ（ただし、ｉは２以上ｋ以下の整数）番目のコンテンツ関係者についての前記電子署名作成処理は、第（ｉ-１）番目のコンテンツ関係者の電子署名の値に依存して定まる値を、第ｉ番目のコンテンツ関係者の秘密鍵で暗号化し、第ｉ-１番目のコンテンツ関係者の電子署名とする処理であることを特徴とするコンテンツ埋め込み情報の処理方法によれば、電子署名の値に依存して定まる値をｎビットとすれば、ｎビットのデータをコンテンツに埋め込むだけで、ｋ人のコンテンツ関係者を検証できる情報をコンテンツに埋め込むことができる。

【００５８】また、前記課題を達成するために、本発明は、たとえば、情報開示者と情報閲覧者の双方が信頼する管理者によって管理されていて、真正性を確認可能なマルチメディアデータを、情報開示者は自己が公開する情報に対して付加し、情報閲覧者は該マルチメディアデータの真正性が確認されたかどうかに応じて前記情報の真正性を確認することを特徴とする情報の認証方法。を提供する。

【００５９】このような方法では、情報の真正性は、たとえば、情報に付加されたマルチメディアデータに対する、全ての関与者が信頼する管理者の真正性の確認に応じて判定される。

【００６０】具体的には、たとえば、Ｗｅｂページを閲覧するユーザが、そのＷｅｂページに貼り付けられた画像データが明示する情報（ユーザが見た目から判断するであろう情報）が真正なものであるか否か、すなわち、画像データ自体が本物であるか否か、さらには、そのＷｅｂページに当該画像データを貼り付けているという事実が、前記画像データが明示する該画像データの管理者に認められたものであるか否かを管理者が認証するか否かに応じて、Ｗｅｂページの真正性を判定する。

【００６１】なお、このような方法において、必要に応じて、上記マルチメディアデータの真正性が確認された場合に上記情報閲覧者に対して当該情報を提供するようにしてもよい。具体的には、たとえば、前記Ｗｅｂページ例では、上記画像データが真正なものであると確認された場合に、当該Ｗｅｂページを表示するように、情報をフィルタリングするようにしてもよい。

【００６２】また、前記課題達成のために本発明は、電子計算機を用いて、電子データに当該電子データを認証するための認証用データを含めた認証可能電子データを作成する方法であって、電子データの利用時に利用者が認知可能な出力を行うマーク用データを生成するステップと、前記マーク用データに所定の情報を電子透かしとして埋め込んだ、透かし入りマーク用データを生成するステップと、生成した透かし入りマーク用データを、前記電子データに含め、前記認証可能電子データを生成するステップとを有することを特徴とする方法を提供する。

【００６３】ここで、このような方法において、前記所定の情報は、前記電子データを所定のハッシュ関数で評価したハッシュ値であってもよい。

【００６４】また、前記所定の情報は、前記電子データを所定の関数で評価した評価値を、所定の公開鍵暗号法に従った秘密鍵で暗号化した電子署名であってもよい。

【００６５】これらのような方法によれば、透かし入りマーク用データに電子透かしとして埋め込まれた情報より、そのマークの真正性を認証可能となる。また、さらに、ハッシュ値を電子透かしとして埋め込む場合は、そのマークがその電子データに対して与えられたことを認証することができる。また、さらに、電子署名を電子透かしとして埋め込む場合には、さらに、そのマークを保証する個人／機関をも認証することができるようにな

る。

【００６６】また、本発明は、この他、前記各方法を実現するためのシステムや装置を提供する。

【００６７】例を挙げれば、たとえば、配布するコンテンツを出力する配布側装置と、配布されたコンテンツを入力する受領側装置とを有するコンテンツ配布システムであって、配布側装置は、配布するコンテンツを暗号化する暗号化手段を備え、受領側装置は、配布されたコンテンツを復号化する復号化手段と、受領側装置の利用者の、公開鍵暗号体系に従った秘密鍵で、所定の情報を暗号化した暗号情報を作成する署名作成手段と、作成した暗号情報を、復号化したコンテンツに、所定の規則に従って、少なくとも当該所定の規則を用いずに当該暗号情報のみを当該コンテンツから分離できないように埋め込む署名埋め込み手段と、を有することを特徴とするコンテンツ配布システムを提供する。

【００６８】また、このようなコンテンツ配布システムであって、署名作成手段が行う暗号情報の作成および前記署名埋め込み手段の行う暗号情報の埋め込みとを行わずに、前記復号化手段の復号化のみを行うことができないように前記復号化手段と署名作成手段と署名埋め込み手段とは構成されており、かつ、署名作成手段が行う暗号情報の作成および前記署名埋め込み手段の行う暗号情報の埋め込みとを行わずに、前記復号化手段の復号化のみを行うように改変することを困難化するプロテクトが受領側装置に設けられていることを特徴とするコンテンツ配布システムを提供する。

【００６９】また、さらには、これらのコンテンツ配布システムであって、前記配布側装置の暗号化手段は、受領側装置の利用者の公開鍵を用いてコンテンツを暗号化し、前記受領側装置の復号化手段は、配布側装置の利用者の秘密鍵を用いて暗号化されたコンテンツを復号化することを特徴とするコンテンツ配布システムを提供する。

【００７０】なお、これらのコンテンツ配布システムに検証装置を備え、当該検証装置は、暗号情報が埋め込まれたコンテンツから、暗号情報を抽出する署名抽出手段と、抽出した暗号情報を、コンテンツの関係者の公開鍵で復号化した結果が、前記所定の情報と一致するかを検証する署名検証手段と、を有するようにしてもよい。

【００７１】また、これらのコンテンツ配布システムにおいては、受領側装置の署名作成手段は、復号化したコンテンツの内容に依存した値をとる情報を前記所定の情報とし、当該所定の情報を、受領側装置の利用者の、公開鍵暗号体系に従った秘密鍵で暗号化した、当該利用者の当該コンテンツに対する電子署名を、前記暗号情報として作成するようにしてもよい。

【００７２】また、本発明は、たとえば、コンテンツに署名を施すデータ処理装置であって、コンテンツをハッシュ関数で評価したハッシュ値を算出し、算出したハッシュ値を、当該データ処理装置の利用者の、公開鍵暗号体系に従った秘密鍵で暗号化し、電子署名とする電子署名作成手段と、作成した電子署名を電子透かしとして、コンテンツに埋め込む電子透かし作成手段とを有することを特徴とするデータ処理装置を提供する。

【００７３】また、本発明は、たとえば、認証可能電子データを生成する生成側装置と、認証可能電子データの認証する認証側装置から構成されるシステムであって、生成側装置は、電子データの利用時に利用者が認知可能な出力を行うマーク用データを生成する手段と、前記マーク用データに所定の情報を電子透かしとして埋め込んだ、透かし入りマーク用データを生成する手段と、生成した透かし入りマーク用データを、前記電子データに含め、前記認証可能電子データを生成する手段とを有し、前記認証側装置は、前記認証可能電子データから前記マーク用データを切り出す手段と、切り出した前記マーク用データから電子透かしとして埋め込まれた前記所定の情報を抽出する手段と、抽出した情報に基づいて電子データを認証する手段とを有するシステムを提供する。

【００７４】より具体的には、たとえば、前記認証可能電子データは、マーク用データを含んだwebページであり、前記認証側装置では、当該webページ及び、当該webページ閲覧時にマーク用データによって出力される内容が示す事項の認証を、マーク用データに電子透かしとして埋め込まれた情報に基づいて行う。なお、この場合、前記認証可能電子データであるwebページを生成する装置／機関と、このwebページを公開する装置／機関は異なる装置であってよい。また、この場合、webページを公開する装置／機関よりの依頼に応じて、前記認証可能電子データであるwebページを生成する装置／機関が前記認証可能電子データであるwebページを作成するようにしてよい。

【００７５】また、本発明は、前記各方法を電子計算機に実施させるためのプログラムを記憶した記憶媒体をも提供する。

【００７６】例を挙げれば、たとえば、電子計算機によって実行されるプログラムを記憶した、電子計算機読み取り可能な記憶媒体であって、前記プログラムは、電子データの利用時に利用者が認知可能な出力を行うマーク用データを生成するステップと、前記マーク用データに所定の情報を電子透かしとして埋め込んだ、透かし入りマーク用データを生成するステップと、生成した透かし入りマーク用データを、前記電子データに含め、前記認証可能電子データを生成するステップと、を電子計算機に実行させるプログラムであることを特徴とする記憶媒体を提供する。

【００７７】また、たとえば、電子計算機によって実行されるプログラムを記憶した、電子計算機読み取り可能な記憶媒体であって、前記プログラムは、

【００７８】

【発明の実施の形態】以下、本発明の実施形態について説明する。

【００７９】まず、復号的でない電子データについて、電子データと個人／機関との関係を、より高い信頼性をもって認証可能とする実施形態を、第１、第２、第３実施形態として説明する。

【００８０】まず、第１の実施形態について説明する。

【００８１】本第１実施形態では、電子データと個人／機関との関係を認証可能とする例として、電子データであるコンテンツの不正コピーを防止する目的のために、コンテンツとコンテンツの購入者との関係を認証可能とする場合を例にとり説明する。ただし、電子データと個人／機関との関係を認証可能とする目的に応じて、本第１実施形態は、電子データとの関係を認証可能とする個人／機関を、コンテンツの購入者ではなく、コンテンツの権利者、コンテンツの販売者、コンテンツを取り扱う中間業者などとするように修正してよい。また、本第１実施形態および後述する第２、第３実施形態では、コンテンツがイメージデータである場合を例にとるが、これは、コンテンツが他の種類のデータ、たとえば、テキストデータやドロウイングデータやオウディオデータやビデオデータであるように修正してよい。

【００８２】まず、本実施形態に係るコンテンツ配布システムの構成を図１に示す。

【００８３】図示するように、コンテンツ配布システムは電子データであるコンテンツを配布するプロバイダー装置１００と、コンテンツの配布を受ける通常複数の購入者装置２００より構成される。

【００８４】プロバイダー装置１００と購入者装置２００の間のコンテンツや、その他の情報のやりとりは、プロバイダー装置１００と購入者装置２００を結ぶネットワーク１０を介して行われる。ただし、ネットワーク１０は必ずしも必要ではなく、プロバイダー装置１００と購入者装置２００の間のコンテンツや、その他の情報のやりとりは、当該情報を記憶したフロッピーディスクなどの記憶媒体の運送、郵送などによってもよい。

【００８５】図２に、プロバイダー装置１００と購入者装置２００の構成を示す。

【００８６】図示するように、プロバイダー装置１００は、処理部１１０と記憶部１２０よりなり、処理部１１０は、入出力を担う入出力部１１１、プロバイダー装置１００内の各部の制御を行う制御部１１２、電子署名が埋め込まれたコンテンツから電子署名を抽出する署名抽出部１１３、電子署名を検証する署名検証部１１４、コンテンツを暗号化する暗号化部１１５、各購入者装置２００との間の送受信を担う送受信部１１６よりなる。また、記憶部１２０は、コンテンツ１２１や検証鍵１２２を記憶する。ここで、検証鍵１２２が、従来の技術の欄で説明した公開鍵に相当する。

【００８７】また、図示するように、購入者装置２００は、処理部２１０と記憶部２２０よりなる。また、処理部２１０は、入出力を担う入出力部２１１、購入者装置２００内の各部の制御を行う制御部２１２、プロバイダー装置１００との間の送受信を担う送受信部２１３、暗号化されたコンテンツの復号を行う復号化部２１４、電子署名を作成する署名生成部２１５、電子署名をコンテンツに埋め込む署名埋め込み部２１６、署名鍵（秘密鍵）と検証鍵（公開鍵）を作成する鍵生成部２１７よりなる。また、記憶部２２０は、電署名鍵２２１や署名入りコンテンツ２２２を記憶する。ここで署名鍵２２１が、従来の技術の欄で説明した秘密鍵に相当する。

【００８８】ここで、プロバイダー装置１００や購入者装置２００は、図３に示すように、ＣＰＵ３０１や、主記憶３０２、ハードディスク装置である外部記憶装置３０３b、他の外部記憶装置である３０３ｂ、通信制御装置３０４、キーボードやポインティングデバイスなどの入力装置３０５、表示装置などの出力装置３０６などを備えた、一般的な構成を有する電子計算機上に構築することができる。

【００８９】この場合、プロバイダー装置１００の処理部１１０、および、処理部１１０の内部の各部は、ＣＰＵ３０１が主記憶３０２にロードされたプログラムを実行することにより電子計算機上に具現化されるプロセスとして実現される。また、この場合、主記憶３０２や外部記憶装置３０３a、bが、プロバイダー装置１００の記憶部１２０として使用される。また、同様に、購入者装置２００の処理部２１０、および、処理部２１０の内部の各部は、ＣＰＵ３０１が主記憶３０２にロードされたプログラムを実行することにより電子計算機上に具現化されるプロセスとして実現される。また、この場合、主記憶３０２や外部記憶装置３０３が、購入者装置２００の記憶部２２０として使用される。

【００９０】前述した主記憶３０２にロードされＣＰＵ３０１によって実行されることにより、電子計算機上にプロバイダー装置１００と購入者装置２００を構成するためのプログラムは、予め、外部記憶装置３０３ｂに記憶され、必要に応じて主記憶３０２にロードされ、ＣＰＵ３０１によって実行される。または、可搬型の記憶媒体３０７、たとえば、CD-ROMを扱う外部記憶装置３０３aを介して、直接、必要に応じて、可搬型の記憶媒体３０７から主記憶３０２にロードされ、ＣＰＵ３０１によって実行される。もしくは、一旦、可搬型の記憶媒体を扱う外部記憶装置３０３aを介して、可搬型の記憶媒体３０７から、ハードディスク装置などの外部記憶装置３０３b上にインストールされた後、必要に応じて主記憶３０２にロードされ、ＣＰＵ３０１によって実行される。

【００９１】以下、プロバイダー装置１００と購入者装置２００の行う処理の詳細を、コンテンツの配布から不正コピーの発見までの時間的流れに沿って説明する。

【００９２】まず、コンテンツの配布に先立ち、購入者装置２００の制御部２１２の制御下で鍵生成部２１７は、署名鍵と検証鍵を生成する。この生成は、従来の秘密鍵と公開鍵の生成と同じように行う。ここでは、秘密鍵を署名鍵と、公開鍵を検証鍵と呼ぶ。

【００９３】次に、鍵生成部２１７は生成した署名鍵を記憶部２２０に記憶すると共に、生成した検証鍵を制御部２１２に渡す。制御部２２１は、送受信部２１３を介してプロバイダー装置１００に検証鍵を送る。プロバイダー装置１００において、送受信部１１６で受け取られた検証鍵は、記憶部１２０に記憶される。

【００９４】以上の処理が終了した以降において、プロバイダー装置１００からコンテンツを購入者装置２００に送る場合の動作は次のようになる。

【００９５】すなわち、制御部１１２は、入出力部１１１と協調して配布するコンテンツを受け入れ、一旦、記憶部１２０に記憶した後、図４に示すように、暗号化部１１５を制御し、記憶したコンテンツ１２１を記憶部１２０に記憶した検証鍵１２２を用いて暗号化し（ステップ４０１）、暗号化したコンテンツを、購入者装置２００に送受信部１１６を介して送信する（ステップ４０２）。

【００９６】一方、暗号化されたコンテンツを受け取った購入者装置１００では、次のような処理を行う。

【００９７】すなわち、図５に示すように、制御部２１２は、送受信部２１３で受け取った暗号化されたコンテンツを復号化部２１４に、記憶部２２に記憶した署名鍵を用いて復号化させ（ステップ５０１）、次に、署名生成部２１５に、復号化したコンテンツの記憶部２２０に記憶した署名鍵を用いた電子署名を生成させる（ステップ５０２）。

【００９８】電子署名の生成は、所定の一方向ハッシュ関数を用いて、復号化したコンテンツの１６０ビットのハッシュ値を算出し、この１６０ビットのハッシュ値を、記憶部２２０に記憶した署名鍵で暗号化することにより行う。

【００９９】電子署名が生成されたならば、制御部２１２は、署名埋込部を制御し、この電子署名を、所定の規則に従って、復号化したコンテンツに不可分となるよう埋め込み（ステップ５０３）、記憶部２２０に記憶する。埋め込みは、たとえば、従来の技術で説明した電子透かしの技術を用いて行う。

【０１００】いま、この後、購入者は、記憶部２２０に記憶された電子署名を埋め込んだコンテンツを不正（コピーする権原を持たずに）にコピーし、第３者に頒布などしてしまった場合を考える。ここで、従来の技術の欄で説明したように、購入者は、電子透かしなどとしてコンテンツにコンテンツと不可分に埋め込んだ電子署名のみをコンテンツから除去して、電子署名なしの完全なコンテンツの不正コピーを作成することはできない。

【０１０１】この不正コピーされた電子署名が埋め込まれたコンテンツが、押収などされた場合、プロバイダー装置１００は、次のようにして、この不正コピーを行った購入者を特定する。

【０１０２】すなわち、図６に示すように、まず、プロバイダー装置１００の制御部１１２は、入出力部１１１と協調して不正コピーされたコンテンツを一旦、記憶部１２０に記憶し、署名抽出部１１３を制御して、不正コピーされたコンテンツから電子署名を抽出する（ステップ６０１）。ここで、プロバイダー装置２００の記憶部１２０には、不正コピーされたコンテンツのオリジナルのコンテンツ（電子署名の埋め込まれていないもの）が記憶されているので、このオリジナルのコンテンツと不正コピーされたコンテンツの差分より電子署名を抽出することができる。もしくは、可能な場合には、電子署名をコンテンツに埋め込んだ規則に従って、電子署名をコンテンツから抽出するようにしてもよい。

【０１０３】次に、制御部１１２は、署名検証部１１４を制御し、抽出した電子署名を、記憶部１２０に記憶した、任意の購入者の検証鍵１２２で復号化し、復号化した値と、購入者装置２００が用いるものと同じ一方向ハッシュ関数で記憶部１２０に記憶しているオリジナルのコンテンツを評価したハッシュ値とを比較することにより、電子署名を検証する（ステップ６０２）。ここで、購入者装置２００が電子署名をコンテンツに埋め込んだ規則がプロバイダー以外に対して秘密化されており、かつ、この規則に基づいて電子署名を、当該電子署名を埋め込んだコンテンツから除去できる場合には、オリジナルのコンテンツに代えて、電子署名を除去したコンテンツを用いるようにしてもよい。

【０１０４】ここで、オリジナルのコンテンツを評価したハッシュ値と復元した電子署名の値が一致すれば、この不正コピーは、電子署名の復号化に用いた検証鍵に対応する購入者に起因するものであると判断することができる。一致しない場合には、さらに他の購入者の検証鍵を用いて不正コピーから抽出した電子署名を復号化し、オリジナルのコンテンツのハッシュ値との一致を検証する。

【０１０５】以上、本発明の第１の実施形態について説明した。

【０１０６】ところで、以上の実施形態において、購入者装置２００において、プロバイダー装置１００より受け取ったコンテンツの復号化のみを行い、電子署名の埋め込みを行わないと、購入者は自身に関する何の情報も埋め込まないコンテンツを手にすることができ、このようなコンテンツの不正コピーからは購入者を特定することができなくなる。

【０１０７】そこで、上述した処理部２１２におけるコンテンツの復号化の処理と電子署名の作成および埋め込みの処理は、一体に行われるように構成する。そして、

これらの処理を分離して行うことのできないようにハードウエア的もしくはソフトウエア的にプロテクトする。具体的には、電子署名の作成および埋め込みの処理が一体に行われるように構成したプログラムをプロバイダーから購入者に提供する。そして、これ以外のプログラムでは、プロバイダー装置１００から送付されたコンテンツを復号化できないようにする。また、プログラムには適当な改変保護プロテクトを設ける。

【０１０８】また、たとえば、前述した復号化の処理と電子署名の作成および埋め込みの処理は、図３に示した電子計算機のＣＰＵ３０１で行うのではなく、プロバイダーが購入者に提供する改変に対するプロテクトを設けたICカード内で行うようにする。この場合、ICカードを電子計算機に接続して用い、ICカードは、電子計算機から送られた暗号化されたコンテンツに対して、電子署名を埋め込んだコンテンツを返すようにする。

【０１０９】また、もちろん、改変に対する保護を施した専用のハードウエア装置によって行うようにしてもよい。

【０１１０】このように第１の実施形態によれば、不正コピーに埋め込まれた、購入者自身しか知らないことが保証される署名鍵（秘密鍵）に依存し、購入者自身しか作成することのできない情報を用いて検証することにより、不正コピーの起因となった購入者を判断するので、不正コピーに埋め込まれた情報と、不正コピーの起因となった購入者との対応の証拠性を向上することができる。また、埋め込む情報として、コンテンツの内容に依存するハッシュ値による電子署名を用いるので、不正コピーに埋め込まれた電子署名が示す購入者とコンテンツとの対応性の証拠性も向上することができる。

【０１１１】ただし、埋め込まれた情報がコンテンツと不可分であることを前提とすれば、コンテンツの内容に依存するハッシュ値による電子署名ではなく、たとえば、プロバイダー装置１００と購入者装置２００に対して公開されたデータ、たとえば、購入者名などのテキストのハッシュ値による電子署名を用いても、ある程度、以上の効果を達成することができる。

【０１１２】以下、本発明の第２の実施形態について説明する。

【０1'1３】本第２実施形態および後述する第３実施形態では、電子データと個人／機関との関係を認証可能とする例として、電子データであるコンテンツの複数の権利者の表示を目的として、コンテンツとコンテンツの複数権利者との関係を認証可能とする場合を例にとり説明する。ただし、電子データと個人／機関との関係を認証可能とする目的に応じて、本第２実施形態および後述する第３実施形態は、電子データとの関係を認証可能とする個人／機関を、複数のコンテンツの権利者ではなく、コンテンツの複数の購入者、コンテンツの複数の販売者、コンテンツを取り扱う複数の中間業者、もしくは、権利者と購入者の組み合わせなどの異なる種類の個人／機関の組み合わせとするように修正してよい。

【０１１４】さて、本第２実施形態は、複数の著作権者などの、配布するコンテンツの複数の権利者の電子署名をコンテンツに埋め込んだ配布コンテンツを作成する配布コンテンツ作成システムについてのものである。

【０１１５】図７に、配布コンテンツ作成システムの構成を示す。

【０１１６】図示するように、配布コンテンツ作成システムは、１または複数のコンテンツを配布するプロバイダー装置１００と、コンテンツの著作権者などの権利者が使用する複数の権利者装置７００より構成される。プロバイダー装置１００と権利者装置７００の間のコンテンツや、その他の情報のやりとりは、プロバイダー装置１００と権利者装置７００を結ぶネットワーク１０を介して行われる。ただし、ネットワーク１０は必ずしも必要ではなく、プロバイダー装置１００と権利者装置７００の間のコンテンツや、その他の情報のやりとりは、当該情報を記憶したフロッピーディスクなどの記憶媒体の運送、郵送などによってもよい。また、この配布コンテンツ作成システムのプロバイダー装置１００、図１に示したコンテンツ配布システムのプロバイダー装置１００を同じプロバイダー装置とすることにより、両システムを一体化するようにしてもよい、図８に、この場合のプロバイダー装置１００と、権利者装置７００の構成を示す。

【０１１７】図示するように、プロバイダー装置１００は、先に図２に示したプロバイダー装置と同じ構成を備えており、権利者装置７００は図２に示した購入者装置２００と同じ構成を備えている。また、第１実施形態と同様に、プロバイダー装置１００も、権利者装置７００も、図３に示したような電子計算機を用いて実現できる。

【０１１８】さて、このような配布コンテンツシステムにおいて、配布するコンテンツの複数の権利者の電子署名をコンテンツに埋め込んだ配布コンテンツを作成する処理は次の手順によって行われる。

【０１１９】ただし、プロバイダー装置１００自身の署名鍵と検証鍵が既に生成されており、プロバイダー装置１００の検証鍵が各権利者装置に配布されているものとする。また、各権利者装置７００は、プロバイダー装置１００へのコンテンツや各種情報を、プロバイダー装置１００の検証鍵で暗号化して送付し、プロバイダー装置１００は送付された情報をプロバイダー装置１００署名鍵で復号化して利用するものとする。なお、この各権利者装置７００からプロバイダー装置１００へ送付する情報についての暗号化、復号化に関わる構成は、プロバイダー装置７００から権利者装置７００や前述した購入者装置２００へ送付する情報についての暗号化、復号化に関わる構成と同じであるので、図７では図示を省略して

いる。

【０１２０】さて、このような状況のもと、まず、配布コンテンツの作成に先立ち、権利者装置７００は、制御部７１２の制御下で鍵生成部７１７は、署名鍵と検証鍵を生成する。この生成は、従来の秘密鍵と公開鍵の生成と同じように行う。

【０１２１】次に、鍵生成部７１７は生成した署名鍵を記憶部７２０に記憶すると共に、生成した検証鍵を制御部７１２に渡す。制御部７２１は、送受信部７１３を介してプロバイダー装置１００に検証鍵を送る。プロバイダー装置１００において、送受信部１１６で受け取られた検証鍵は、記憶部１２０に記憶される。

【０１２２】以上の処理が終了した以降において、プロバイダー装置１００は、複数の権利者の全てについて、順次、権利者の権利者装置７００にコンテンツを送付し、当該権利者装置から返却されたコンテンツを次の権利者の権利者装置７００に送付する処理を行う。

【０１２３】すなわち、制御部７１２は、入出力部７１１と協調して配布するコンテンツを受け入れ、一旦、記憶部７２０に記憶した後、暗号化部７１５を制御し、記憶したコンテンツ７２１を記憶部７２０に記憶した、コンテンツを送付しようとする権利者装置７００から送られた検証鍵７２２を用いて暗号化し、暗号化したコンテンツを、権利者装置７００に送受信部７１５を介して送信する。そして、権利者装置７００から、当該プロバイダー装置１００自身の検証鍵で暗号化されたコンテンツが返却されたならば、これを、当該プロバイダー装置１００の署名鍵で復号化し、次にコンテンツを送付する権利者装置７００の検証鍵で暗号化し、当該次の権利者装置７００に送付する。また、コンテンツの送付の際に、第１番目にコンテンツを送付した権利者装置以外の権利者装置７００には、短縮電子署名の使用の指示を添付する。

【０１２４】一方、プロバイダー装置１００から暗号化されたコンテンツを受け取った権利者装置７００では、次のような処理を行う。

【０１２５】すなわち、制御部７１２は、送受信部７１３で受け取った暗号化されたコンテンツを復号化部７１４に、記憶部７２０に記憶した署名鍵を用いて復号化させ、次に、署名生成部７１５に、復号化したコンテンツの記憶部７２０に記憶した署名鍵を用いた電子署名を生成させる。

【０１２６】電子署名の生成は、所定の一方向ハッシュ関数を用いて、復号化したコンテンツの１６０ビットのハッシュ値を算出し、この１６０ビットのハッシュ値を、記憶部７２０に記憶した署名鍵で暗号化することにより行う。ただし、送付されたコンテンツに短縮電子署名の使用の指示が添付されている場合には、８０ビットのハッシュ値を算出し、この８０ビットのハッシュ値を、記憶部７２０に記憶した署名鍵で暗号化することにより電子署名を作成する。

【０１２７】次に、電子署名が生成されたならば、制御部７１２は、署名埋込部を制御し、この電子署名を、所定の規則に従って、復号化したコンテンツに不可分となるよう埋め込む。埋め込みは、たとえば、従来の技術で説明した電子透かしの技術を用いて行う。そして、電子署名を埋め込んだコンテンツを、送受信部７１３を介して、プロバイダー装置１００に送付することにより返却する。

【０１２８】この結果、最終的に、プロバイダー装置１００に、最後の権利者装置７００から返却されたコンテンツには、次のように順次、各権利者の電子署名が埋め込まれることになる。

【０１２９】すなわち、コンテンツDに対して第i番目の権利者の電子署名が埋め込まれたコンテンツをFi（D）で表すこととすると、まず、第１の権利者はオリジナルのコンテンツの１６０ビットのハッシュ値である電子署名をコンテンツに埋め込みF1（D）とする。次に、第２の権利者は第１の権利者の電子署名が埋め込まれたコンテンツの８０ビットのハッシュ値である電子署名をコンテンツに埋め込み、F2（F1（D））とする。以下同様に、第ｎ番目の権利者は、第１から第１-ｎ番目の権利者の電子署名が埋め込まれたコンテンツの８０ビットのハッシュ値である電子署名をコンテンツに埋め込み、Fn（Fn-1（Fn－2（.....（F2（F1（D））...）とする。

【０１３０】プロバイダー装置１００は、最終的に最後の権利者から返却された、以上のように順次各権利者の電子署名が埋め込まれたコンテンツを配布コンテンツとする。

【０１３１】このように、本第２実施形態では、第２番目の権利者以降の権利者の電子署名に用いるハッシュ値のビット数を、第１番目の権利者が電子署名に用いるハッシュ値のビット数の半分としている。これは、既に、電子署名が施されたコンテンツの偽造は、電子署名が施されていないコンテンツを偽造する場合に比べ困難となることから、第２番目以降の権利者の電子署名に用いるハッシュ値のビット数を、第１番目の権利者が電子署名に用いるハッシュ値のビット数の半分としても、そのセキュリティは、各権利者が１６０ビットの電子署名をオリジナルのコンテンツに施す場合と同様に守られることによるものである。

【０１３２】電子署名を埋め込んだコンテンツよりの各権利者の検証は、第１実施形態における購入者の検証と同様に行う。

【０１３３】以下、本発明の第３実施形態を説明する。

【０１３４】本第３実施形態は、第２実施形態における各権利者の電子署名の埋め込の方法を修正したものである。

【０１３５】すなわち、第３実施形態では、第１の権利

者は、第２実施形態と同様、プロバイダー装置１００から送られたコンテンツのハッシュ値を暗号化して電子署名を生成する。しかし、第１の権利者の権利者装置７００は、電子署名をコンテンツに埋め込まずに、電子署名をプロバイダー装置１００に返却する。プロバイダー装置１００は、返却された第１の権利者の電子署名を、第２の権利者の権利者装置７００に送付する。第２の権利者装置７００は、送付された第１の権利者の電子署名のハッシュ値を暗号化して自身の電子署名とする。以下、同様に、第２番目以降の権利者の権利者装置７００は、前の権利者の電子署名のハッシュ値を暗号化して自身の電子署名とする。

【０１３６】そして、最後の権利者の権利者装置７００の電子署名を受け取ったプロバイダー装置７００は、これを、オリジナルのコンテンツに電子透かしなどとして埋め込み配布コンテンツとする。

【０１３７】ただし、最後の権利者の権利者装置７００にプロバイダー装置１００からオリジナルのコンテンツを送り、最後の権利者の権利者装置７００で最終的な電子署名をコンテンツに埋め込み、これをプロバイダー装置に返却するようにしてもよい。

【０１３８】また、次のように、電子署名の埋め込みを行うようにしてもよい。すなわち、第１番目の権利者の権利者装置７００において、コンテンツのハッシュ値を暗号化した電子署名をコンテンツに埋め込んでプロバイダー装置１００を介して第２番目の権利者の権利者装置７００に送付するようにし、第２番目以降の権利者の権利者装置７００は、受け取った電子署名が埋め込まれたコンテンツから前の権利者の電子署名を抽出し、抽出した電子署名のハッシュ値を暗号化した電子署名を自身の電子署名として作成し、これを、プロバイダー装置１００から別途受け取ったオリジナルのコンテンツに埋め込む。もしくは、自身の電子署名に、前の権利者の電子署名が埋め込まれたコンテンツ中の電子署名を入れ替える。そして、自身の電子署名を埋め込んだコンテンツを、プロバイダー装置１００を介して次の権利者の権利者装置７００に送付する。

【０１３９】電子署名を埋め込んだコンテンツよりの各権利者の検証は、従来の技術の欄で説明したApplied Cryptography, Jhon Wilsy & SOns, Inc. (1996), pp 39-41における場合と同様である。但し、最後に署名した権利者の電子署名は、電子署名が埋め込まれたコンテンツから抽出する。

【０１４０】以上、本発明の第３実施形態について説明した。

【０１４１】第２、第３の実施形態によれば、第２番目以降の権利者の電子署名に用いるハッシュ値を第１番目のものの半分としたり、第２番目以降の権利者の電子署名の対象を前の権利者の電子署名とすることに、より少ない情報量の情報の埋め込みによって、複数の権利者の電子署名を埋め込むことができるので、コンテンツの情報の質の劣化を少なくすることができる。ただし、埋め込まれた情報がコンテンツと不可分であることを前提とすれば、コンテンツの内容に依存するハッシュ値による電子署名ではなく、たとえば、プロバイダー装置１００と権利者装置７００に対して公開されたデータ、たとえば、権利者名などのテキストのハッシュ値による電子署名を用いてもよい。

【０１４２】以下、電子データと個人／機関との関係を認証可能とすると共に、電子データとの関係が認証可能な個人／機関と一致することが保証されるように、当該個人／機関を電子データによって利用者に直接提示する実施形態を、第４から第８実施形態として説明する。

【０１４３】なお本第４実施形態から第８実施形態においては、電子データとしてwebページを例にとり、webページとの関係を認証可能とする個人／機関がクレジット会社であり、そのクレジット会社のマークを販売者が自webページ植えで使用する場合を例にとり説明する。ただし、これらは一例であり、以下に説明する第４実施形態から第８実施形態は、電子データと個人／機関との関係を認証可能とする目的に応じて、webページとの関係を認証可能とする個人／機関を、webページの発信者や、webページとの関係を承認する何らかの個人／機関（たとえば、webページの評価、推奨機関）など、クレジット会社以外のものに置き換えてもよい。また、同様に、販売者は、webページとの関係を認証可能とする個人／機関のマークを使用するwebページ提供者に置き換えてよい。

【０１４４】また、本第４実施形態から第８実施形態においては、電子データによる利用者への直接提示を、電子データとの関係を認証可能な個人／機関のロゴマーク（イメージデータ）を用いて行う場合を例にとるが、これは、電子データによる利用者への直接提示を、電子データ利用時に利用者が知覚可能な他の種類のデータ、たとえば、テキストデータやドロウイングデータやオウディオデータやビデオデータを用いて行うように修正してもよい。または、電子データと認証可能な関係を持つ者を直接表すものではなく、その者の電子データに対する特定の個人／機関の評価結果などを表すマークを用いるように修正してもよい。

【０１４５】まず、第４の実施形態について説明する。

【０１４６】図９に、本第４実施形態に係る認証システムの構成を示す。

【０１４７】図示するように、認証システムは、商品を買う消費者１１００-１～１１００-ｎ（以下、単に消費者１１００とも称する）と、商品を販売する販売者１１１０と、各種マークを管理するマーク管理者１１２０とが利用するシステムであって、図９に示すように、消費者端末１１０１-１～１１０１-ｎ（以下、単に消費者端末１１０１とも称する）と、販売者端末１１１２と、W

WWWサーバ１１１３と、マーク管理サーバ１１２２とが、インターネットのような通信網１１４０を介して、互いに接続されて構成されている。ここで、マーク管理者１１２０は、本システムを利用する全てのマーク所有者（販売者１１１０など）にとって信頼できる公正な機関である。ただし、マーク所有者が自己のマークを管理するマーク管理者１２０を兼ねるようにしてもよく、この場合、販売者端末１１１２と、WWWサーバ１１１３と、マーク管理サーバ１１２２とは、同一のマシンを用いて構成するようにしてもよい。

【０１４８】消費者端末１１０１は、消費者１１００が使用する端末である。消費者端末１１０１は、消費者１１００に文書データや画像データなどを表示する表示装置１１０２と、消費者１１００がデータや命令などを入力するための入力装置１１０３-1や１１０３-2（以下、単に入力装置１１０３とも称する）を備えている。消費者１１００は、消費者端末１１０１および通信網１１４０を介して、販売者１１１０やマーク管理者１１２０とデータのやり取りを行う。

【０１４９】販売者端末１１１２は、販売者１１１０が使用する端末である。販売者１１１０は、販売者端末１１１２を使って、自己が管理する販売店１１１１のＷｅｂページを作成したり、マーク管理者１１２０とデータのやり取りを行ったりする。

【０１５０】WWWサーバ１１１３は、後述のWWWサーバプログラム１４０７ｂが動作するサーバであり、消費者端末１１０１から同じく後述のブラウザプログラム１２０４ｂによるアクセスがあった場合に、ＷｅｂページＤＢ１１１４に格納された当該Ｗｅｂページを送信する。該送信されたＷｅｂページは消費者端末１１０１の表示装置１１０２に表示される。

【０１５１】マーク管理サーバ１１２２は、販売者１１１０からの要求に応じてマークを送付する。さらに、消費者１１００からの要求に応じて、該マークの真正性、すなわち、当該要求を受け付ける以前に、自マーク管理サーバ１２２から販売店１１１０に送付されたものであるかどうかを確認し、その結果を消費者１１００に返送する。

【０１５２】次に、本第４実施形態の認証システムを構成する消費者端末１１０１、販売者端末１１１２、WWWサーバ１１１３、およびマーク管理サーバ１１２２について説明する。

【０１５３】図１０は、消費者端末１１０１のハードウェア構成を示す図である。

【０１５４】本第１実施形態の消費者端末１１０１のハードウェア構成は、図９に示すように、表示装置１１０２と、入力装置１１０３と、通信網インタフェース１２０１と、記憶装置１２０２と、中央処理装置（ＣＰＵ）１２０３と、一時記憶装置（メモリ）１２０４とが、バス１２００によって互いに接続されて構成されている。

【０１５５】表示装置１１０２は、消費者端末１１０１を使用する消費者１１００にメッセージなどを表示するために用いられるものであり、ＣＲＴや液晶ディスプレイなどで構成される。

【０１５６】入力装置１１０３は、消費者端末１１０１を使用する消費者１１００がデータや命令などを入力するために用いられるものであり、キーボードやマウスなどで構成される。

【０１５７】通信網インターフェース１２０１は、通信網１１４０を介してWWWサーバ１１１３や、マーク管理サーバ１１２２とデータのやり取りを行うためのインタフェースである。

【０１５８】記憶装置１２０２は、消費者端末１１０１で使用されるプログラムやデータを永続的に記憶するために用いられるものであり、ハードディスクやフロッピーディスクなどで構成される。

【０１５９】ＣＰＵ１２０３は、消費者端末１１０１を構成する各部を統括的に制御したり、様々な演算処理を行ったりする。

【０１６０】メモリ１２０４には、オペレーティングシステム１２０４ａ（以下、単にＯＳ１２０４ａとも称する）や、ブラウザプログラム１２０４ｂ、あるいは真正性確認プログラムＡ１２０４ｃといった、ＣＰＵ１２０３が上記の処理をするために必要なプログラムなどが一時的に格納される。

【０１６１】ここで、ＯＳ１２０４ａは、消費者端末１１０１全体の制御を行うために、ファイル管理やプロセス管理、あるいはデバイス管理といった機能を実現するためのプログラムである。

【０１６２】ブラウザプログラム１２０４ｂは、消費者端末１１０１がWWWサーバ１１１３と通信し、ＷｅｂページＤＢ１１１４に格納されたＷｅｂページをダウンロードするためのプログラムである。

【０１６３】真正性確認プログラムＡ１２０４ｃは、消費者端末１１０１がマーク管理プログラムＡ１１２２と通信し、WWWサーバ１１１３からダウンロードしたＷｅｂページに貼り付けられたマークの真正性を確認するためのプログラムである。

【０１６４】図１１は、販売者端末１１１２のハードウェア構成を示す図である。

【０１６５】本第４実施形態の販売者端末１１１２のハードウェア構成は、図１１に示すように、表示装置１３０１と、入力装置１３０２と、通信網インタフェース１３０３と、記憶装置１３０４と、中央処理装置（ＣＰＵ）１３０５と、一時記憶装置（メモリ）１３０６とが、バス１３００によって互いに接続されて構成されている。

【０１６６】表示装置１３０１は、販売者端末１１１２を使用する販売者１１１０にメッセージなどを表示するために用いられるものであり、ＣＲＴや液晶ディスプレ

イなどで構成される。

【０１６７】入力装置１３０２は、販売者端末１１１２を使用する販売者１１１０がデータや命令などを入力するために用いられるものであり、キーボードやマウスなどで構成される。

【０１６８】通信網インターフェース１３０３は、通信網１１４０を介してWWWサーバ１１１３や、マーク管理サーバ１１２２とデータのやり取りを行うためのインタフェースである。

【０１６９】記憶装置１３０４は、販売者端末１１１２で使用されるプログラムやデータを永続的に記憶するために用いられるものであり、ハードディスクやフロッピーディスクなどで構成される。

【０１７０】ＣＰＵ１３０５は、販売者端末１１１２を構成する各部を統括的に制御したり、様々な演算処理を行ったりする。

【０１７１】メモリ１３０６には、ＯＳ１３０６ａや、Ｗｅｂページ作成プログラム１３０６ｂ、あるいはマーク取得プログラム１３０６ｃといった、ＣＰＵ１３０５が上記の処理をするために必要なプログラムなどが一時的に格納される。

【０１７２】ここで、ＯＳ１３０６ａは、販売者端末１１１２全体の制御を行うために、ファイル管理やプロセス管理、あるいはデバイス管理といった機能を実現するためのプログラムである。

【０１７３】Ｗｅｂページ作成プログラム１３０６ｂは、販売者１１００がＷｅｂページを作成する処理と、WWWサーバ１１１３と通信し、作成したＷｅｂページをＷｅｂページＤＢ１１１４に格納する処理とを行うためのプログラムである。

【０１７４】マーク取得プログラム１３０６ｃは、販売者端末１１１２がマーク管理プログラムＡ１１２２と通信し、Ｗｅｂページに貼り付けるマークを取得するためのプログラムである。

【０１７５】図１２は、WWWサーバ１１１３のハードウェア構成を示す図である。

【０１７６】本第４実施形態のWWWサーバ１１１３のハードウェア構成は、図１２に示すように、表示装置１４０１と、入力装置１４０２と、通信網インタフェース１４０３と、ＷｅｂページＤＢインターフェース１４０４と、記憶装置１４０５と、中央処理装置（ＣＰＵ）１４０６と、一時記憶装置（メモリ）１４０７とが、バス１４００によって互いに接続されて構成されている。

【０１７７】表示装置１４０１は、WWWサーバ１１１３を使用する販売者１１１０にメッセージなどを表示するために用いられるものであり、ＣＲＴや液晶ディスプレイなどで構成される。

【０１７８】入力装置１４０２は、WWWサーバ１１１３を使用する販売者１１１０がデータや命令などを入力するために用いられるものであり、キーボードやマウスなどで構成される。

【０１７９】通信網インターフェース１４０３は、通信網１１４０を介して消費者端末１１０１や、販売者端末１１１２とデータのやり取りを行うためのインタフェースである。

【０１８０】ＷｅｂページＤＢインターフェース１４０４は、ＷｅｂページＤＢ１１１４とデータのやり取りを行うためのインターフェースである。

【０１８１】記憶装置１４０５は、WWWサーバ１１１３で使用されるプログラムやデータを永続的に記憶するために用いられるものであり、ハードディスクやフロッピーディスクなどで構成される。

【０１８２】ＣＰＵ１４０６は、WWWサーバ１１３を構成する各部を統括的に制御したり、様々な演算処理を行ったりする。

【０１８３】メモリ１４０７には、ＯＳ１４０７ａやWWWサーバプログラム１４０７ｂといった、ＣＰＵ１４０６が上記の処理をするために必要なプログラムなどが一時的に格納される。

【０１８４】ここで、ＯＳ１４０７ａは、WWWサーバ１１１３全体の制御を行うために、ファイル管理やプロセス管理、あるいはデバイス管理といった機能を実現するためのプログラムである。

【０１８５】WWWサーバプログラム１４０７ｂは、販売者端末１１１２と通信し、受け取ったＷｅｂページをＷｅｂページＤＢ１１１４に格納する処理と、消費者端末１１０１からブラウザプログラム１２０４ｂによるアクセスがあった場合に、ＷｅｂページＤＢ１１１４に格納されている当該Ｗｅｂページを送信する処理とを行うためのプログラムである。

【０１８６】図１３は、マーク管理サーバ１１２２のハードウェア構成を示す図である。

【０１８７】本第４実施形態のマーク管理サーバ１１２２のハードウェア構成は、図１３に示すように、表示装置１５０１と、入力装置１５０２と、通信網インタフェース１５０３と、マーク管理ＤＢインターフェース１５０４と、記憶装置１５０５と、中央処理装置（ＣＰＵ）１５０６と、一時記憶装置（メモリ）１５０７とが、バス１５００によって互いに接続されて構成されている。

【０１８８】表示装置１５０１は、マーク管理サーバ１１２２を使用するマーク管理者１１２０にメッセージなどを表示するために用いられるものであり、ＣＲＴや液晶ディスプレイなどで構成される。

【０１８９】入力装置１５０２は、マーク管理サーバ１１２２を使用するマーク管理者１１２０がデータや命令などを入力するために用いられるものであり、キーボードやマウスなどで構成される。

【０１９０】通信網インターフェース１５０３は、通信網１１４０を介して消費者端末１１０１や、販売者端末１１１２とデータのやり取りを行うためのインタフェー

スである。

【０１９１】マーク管理ＤＢインターフェース１５０４は、マーク管理ＤＢ１１２３とデータのやり取りを行うためのインターフェースである。該マーク管理ＤＢ１１２３は、マークの種別や、当該マークの有効期限、販売者の識別情報、あるいは販売店のＷｅｂページのＵＲＬなどといったデータを対応づけて管理するものであり、たとえば図１５のようなものである。図１５において、マークに有効期限を設けない場合、また、マーク管理者１２０がただ一つのマークのみを発行する場合には、それぞれに対応する項目、すなわち有効期限やマーク種別などを管理しなくてよいのは明らかである。

【０１９２】記憶装置１５０５は、マーク管理サーバ１１２２で使用されるプログラムやデータを永続的に記憶するために用いられるものであり、ハードディスクやフロッピーディスクなどで構成される。

【０１９３】ＣＰＵ１５０６は、マーク管理サーバ１１２２を構成する各部を統括的に制御したり、様々な演算処理を行ったりする。

【０１９４】メモリ１５０７には、ＯＳ１５０７ａやマーク管理プログラムＡ１５０７ｂといった、ＣＰＵ１５０６が上記の処理をするために必要なプログラムなどが一時的に格納される。

【０１９５】ここで、ＯＳ１５０７ａは、マーク管理サーバ１１２２全体の制御を行うために、ファイル管理やプロセス管理、あるいはデバイス管理といった機能を実現するためのプログラムである。

【０１９６】マーク管理サーバプログラムＡ１５０７ｂは、販売者端末１１１２からマーク送付要求があった場合に、販売者１１１０を確認してマークを送付するか否かを判定した後、送付すべきであると判定した場合にのみ、マーク管理ＤＢ１１２３によって管理されているマークを販売者１１１０に送信する処理と、消費者端末１１０１からマークの真正性確認要求があった場合に、マーク管理ＤＢ１１２３を参照して当該マークの真正性を検証し、その結果を返送する処理とを行うためのプログラムである。

【０１９７】次に、本第４実施形態の認証システムの動作について説明する。

【０１９８】図１４は、販売者１１１０がマーク管理者１１２０からマークを受け取り、該マークを自己のＷｅｂページに貼り付けてから公開した後、消費者１１００が当該Ｗｅｂページを閲覧して、該Ｗｅｂページの真正性を確認する場合の、消費者１１００と販売者１１１０、およびマーク管理者１２０の動作を説明するための図である。

【０１９９】図１４において、消費者１１００が行う処理には消費者端末１１０１が使用され、販売者１１１０が行う処理には販売店端末１１１２およびＷＷＷサーバ１１１３が使用される。また、マーク管理者１１２０が行う処理にはマーク管理サーバ１１２２が使用される。

【０２００】まず、販売者１１１０は、自己のＷｅｂページのＵＲＬやマーク種別などを含むマーク送付要求をマーク管理者１１２０に送る（ステップ１６００）。

【０２０１】要求を受けたマーク管理者１１２０は、当該要求に含まれるマーク種別で指定されたマークを販売者１１１０に対して送付するか否かを判定し（ステップ１６０１）、送付すると判定した場合にのみ、マーク管理ＤＢ１１２３を更新した後（ステップ１６０２）、当該マークを販売者１１１０に送付する（ステップ１６０３）。また、送付しないと判定した場合にはその旨を販売者１１１０に通知する。本第４実施形態での送付するか否かの判定は、販売者１１１０が当該マークを取得する権利を有しているか否か、すなわち当該マークをロゴとして使用しているクレジットカード会社の加盟店であるか否か、ということに基づいて行う。しかし、これは、マークを交付する目的に応じて別の基準を用いてもよい。

【０２０２】マークを受け取った販売者１１１０は、該マークを自己のＷｅｂページに貼り付けてマーク付きＷｅｂページを作成するとともに（ステップ１６０４）、該マークにマーク管理者１１２０へのリンク情報を設定し（ステップ１６０５）、当該Ｗｅｂページを消費者１１００からアクセス可能な状態でＷｅｂページＤＢ１１１４に格納する（ステップ１６０６）。

【０２０３】次に、消費者１１００は、上記ＷｅｂページのＵＲＬを含んだＷｅｂページ送付要求を販売者１１１０に送る（ステップ１６０７）。

【０２０４】要求を受け取った販売者１１１０は、ＷｅｂページＤＢ１１１４を検索し（ステップ１６０８）、当該ＵＲＬに対応したＷｅｂページを消費者１１００に返送する（ステップ１６０９）。

【０２０５】Ｗｅｂページを受け取った消費者１１００は、さらに、表示された（ステップ１６１０）該Ｗｅｂページに貼り付けられたマークをクリックし（ステップ１６１１）、当該ＷｅｂページのＵＲＬなどを含む真正性確認要求をマーク管理者１１２０に送る（ステップ１６１１）。その際、もし、上記マークにマーク管理者１１２０へのリンク情報が正しく設定されていないためにマーク管理者１１２０への真正性確認要求を送れなかった場合には、消費者１１００は、該マークの真正性が確認されなかったもの（にせのマーク）と判断して、全ての処理を終了する。

【０２０６】要求を受け取ったマーク管理者１１２０は、マーク管理ＤＢ１１２３を検索して、当該要求に含まれるＵＲＬで指定された販売者１１１０に対して、すでにマークを送付しているか否か、また、送付している場合、該マークが有効期限内であるかどうかを確認する（ステップ１６１２）。そして、<1>ＵＲＬで指定された販売店１１１０にはマークを発行していない、<2>U

ＲＬで指定された販売店１１１０にマークを発行しているが、すでに有効期限がきれている、〈3〉ＵＲＬで指定された販売店１１１０にマークを発行しており、かつ、そのマークは有効期限内である、といった３種類の結果のいずれか一つを、消費者１１００に送付する（ステップ６１３）。

【０２０７】最後に、上記結果を消費者１１００が確認して全ての処理が終了する（ステップ６１４）。

【０２０８】上記手順において、消費者１１００による真正性の確認は、たとえば、図９に示すように表示装置１１０２に「本物です」（あるいは「にせものです」、「期限切れです」、「リンク情報が正しく設定されていません」）といった吹き出しが表示され、消費者１１００が該吹き出しを見ることによって行われる。しかし、これは、別の表示方法を用いてもよい。また、音などを用いて行ってもよいし、音、表示を組み合わせても良い。

【０２０９】さて、本第４実施形態では、マーク管理者１１２０はマークを受け取る権利がある販売店１１１０にのみマークを送付するようにしている。そして、マークの関連情報（送付した販売者１１１０の識別情報やＷｅｂページのＵＲＬ、マークの有効期限など）をマーク管理ＤＢ１１２３で管理するようにしている。さらに、該マーク管理ＤＢ１１２３を参照し、消費者１１００から送られてきた真正性確認要求に含まれるＵＲＬが示す販売者１１１０に対して、すでにマークを送付しているか否か、また、送付している場合には、そのマークが有効期限内のものであるか否かを確認して、消費者に通知するようにしている。

【０２１０】また、消費者１１００は、Ｗｅｂページに貼り付けられたマークに設定されたリンク情報を使って、マークの真正性をマーク管理者１１２０に確認するようにしている。さらに、マーク管理者１１２０へのリンク情報が正しく設定されていないためにマーク管理者１１２０への真正性確認要求を送れなかった場合には、該マークの真正性が確認されなかったもの（にせのマーク）と判断するようにしている。

【０２１１】したがって、本第４実施形態によれば、不正者が自己のＷｅｂページに、正規販売者のＷｅｂページからコピーしたマークを貼り付けた場合は、マーク管理者が管理するマーク管理ＤＢに不正者のＷｅｂページにマークを送付した記録がないため、真正性確認処理で該マークの真正性が確認されない。結果として販売者のＷｅｂページを閲覧する消費者が、そのＷｅｂページに貼り付けられたマークが明示する情報が真正なものであるか否かを正しく確認することができることになる。

【０２１２】なお、本第４実施形態では、消費者１１００がマークをクリックすることで真正性確認処理が開始されるようにしているが、これは、Ｗｅｂページを受け取ったときに自動的に真正性確認処理が開始されるようにしてもよい。さらに、該処理において真正性が確認された場合に、当該Ｗｅｂページが表示されるようにしてもよい。

【０２１３】また、本第４実施形態では、販売者端末１１２とWWWサーバ１１３とを別マシンとして説明したが、これは同一のマシンであってもよい。

【０２１４】以下、本発明の第５実施形態について説明する。

【０２１５】図１６に、本第５実施形態に係る認証システムの構成を示す。

【０２１６】本第５実施形態の認証システムの構成は、基本的には図９に示したものと同じである。ただし、各消費者端末１８００-１～１８００-ｎ（以下、単に消費者端末１８００とも称する）に、それぞれ公開鍵ＤＢ１８０１-１～１８０１-ｎ（以下、単に公開鍵ＤＢ１８０１とも称する）が接続されている点が異なる。

【０２１７】公開鍵ＤＢ１８１０は、マーク管理者の公開鍵を管理するものであり、たとえば図２０のようなものである。これらの公開鍵は、当該マーク管理者が生成したディジタル署名（以下、単に署名とも称する）を検証する際に用いられる。

【０２１８】図１７は、本第５実施形態の消費者端末１８００のハードウェア構成を示す図である。

【０２１９】本第５実施形態の消費者端末８００のハードウェア構成は、基本的には図１０に示したものと同じである。ただし、公開鍵ＤＢインタフェース１９００を備えている点と、メモリ１９０１上に真正性確認プログラムＢ９０２が格納され、実行される点とが異なる。

【０２２０】公開鍵ＤＢインタフェース１９００は、公開鍵ＤＢ１８０１とデータのやり取りを行うためのインターフェースである。また、真正性確認プログラムＢ１９０２は、マーク管理サーバ１８１０と通信し、マーク管理者１１２０の公開鍵を取得する処理と、該公開鍵を用いて、WWWサーバ１１３からダウンロードしたＷｅｂページに貼り付けられた署名付きマークの真正性を確認する処理とを行うためのプログラムである。

【０２２１】図１８は、本実施形態のマーク管理サーバ１８１０のハードウェア構成を示す図である。

【０２２２】本第５実施形態のマーク管理サーバ１８１０のハードウェア構成は、基本的には図１３に示したものと同じである。ただし、メモリ１１０００上にマーク管理プログラムＢ１１００１が格納され、実行される点が異なる。

【０２２３】マーク管理プログラムＢ１１００１は、消費者端末１８００から公開鍵送付要求があった場合に、自己の公開鍵を送付する処理と、販売者端末１１１２からマーク送付要求があった場合に、販売者１１１０を確認してマークを送付するか否かを判定した後、送付すべきであると判定した場合にのみ、該販売者１１１０のＷｅｂページのＵＲＬを示すデータに秘密鍵を用いて電子

署名を作成し、電子署名とマーク管理ＤＢ１１２３によって管理されているマークとを一纏めにして署名付きマークを作成し、該署名付きマークを販売者１１１０に送信する処理とを行うためのプログラムである。電子署名とマークとを一纏めにすることは、たとえば、前述した電子透かし技術を利用し、マークに電子署名による電子透かしを施すことにより可能となる。電子透かしは、画像データに微少な変更を加えることで、情報を埋め込む技術である。マークは画像データの一種であることから、電子透かしを用いて任意の情報を埋め込むことができる。また、電子透かしには、カラー画像用、白黒画像用、２値画像用などがあるので、各種のマークへの情報埋込みが可能である。しかし、これは別の手法を用いてもよい。なお、マークと電子署名とを一纏めにする手段として電子透かしを用いる場合、マークの視認性さえ阻害しなければ（たとえば、どこのクレジットカード会社のロゴマークだということがわかれば）、マーク自体は多少変形されてもよい。

【０２２４】また、署名に用いる公開鍵暗号方式としては、素因数分解を用いるもの、楕円曲線を用いるものなどが使用可能である。

【０２２５】次に、本第５実施形態の認証システムの動作について説明する。

【０２２６】図１９は、消費者１１００がマーク管理者１１２０の公開鍵を取得した後、販売者１１１０がマーク管理者１１２０からマークを受け取り、該マークを自己のＷｅｂページに貼り付けてから公開し、さらに、消費者１１００が当該Ｗｅｂページを閲覧して、該Ｗｅｂページの真正性を確認する場合の、消費者１１００と販売者１１１０、およびマーク管理者１２１０の動作を説明するための図である。

【０２２７】図１９において、消費者１１００が行う処理には消費者端末１８００が使用され、販売者１１１０が行う処理には販売店端末１１１２およびWWWサーバ１１１３が使用される。また、マーク管理者１１２０が行う処理にはマーク管理サーバ１８１０が使用される。

【０２２８】まず、消費者１１００は、公開鍵送付要求をマーク管理者１１２０に送る（ステップ１１１００）。

【０２２９】要求を受け取ったマーク管理者１１２０は（ステップ１１１０１）、自己の公開鍵を消費者１１００に返送する（ステップ１１１０２）。

【０２３０】マーク管理者１１２０の公開鍵を受け取った消費者１１００は、該公開鍵を公開鍵ＤＢ１８０１に格納する（ステップ１１１０３）。

【０２３１】次に、販売者１１１０は、自己のＷｅｂページのＵＲＬやマーク種別などを含むマーク送付要求をマーク管理者１１２０に送る（ステップ１１１０４）。

【０２３２】要求を受けたマーク管理者１１２０は、当該要求に含まれるマーク種別で指定されたマークを販売者１１１０に対して送付するか否かを判定し（ステップ１１１０５）、送付すると判定した場合にのみ、当該要求に含まれるＵＲＬデータに秘密鍵を用いて署名を施し、該署名とマーク種別で指定されたマークとを一纏めにして署名付きマークを生成する（ステップ１１１０６）。そして、該署名付きマークを販売者１１１０に送付する（ステップ１１１０７）。また、送付しないと判定した場合にはその旨を販売者１１１０に通知する。本実施形態での送付するか否かの判定も、第４の実施形態と同様、販売者１１１０が当該マークを取得する権利を有しているか否か、すなわち当該マークをロゴとして使用しているクレジットカード会社の加盟店であるか否か、ということに基づいて行う。ただし、他の適当な基準を用いてもよい。

【０２３３】署名付きマークを受け取った販売者１１１０は、該署名付きマークを自己のＷｅｂページに貼り付けてマーク付きＷｅｂページを作成し（ステップ１１１０８）、当該Ｗｅｂページを消費者１１００からアクセス可能な状態でＷｅｂページＤＢ１１１４に格納する（ステップ１１１０９）。

【０２３４】次に、消費者１１００は、上記Ｗｅｂページの ＵＲＬを含んだＷｅｂページ送付要求を販売者１１１０に送る（ステップ１１１１０）。

【０２３５】要求を受け取った販売者１１１０は、ＷｅｂページＤＢ１１１４を検索し（ステップ１１１１１）、当該ＵＲＬに対応したＷｅｂページを消費者１１００に返送する（ステップ１１１１２）。

【０２３６】Ｗｅｂページを受け取った消費者１１００が、表示された（ステップ１１１１３）該Ｗｅｂページに貼り付けられた署名付きマークをクリックすると（ステップ１１１１４）、公開鍵ＤＢ１８０１に格納されたマーク管理者１１２０の公開鍵と該ＷｅｂページのＵＲＬとを用いて、該署名付きマークに含まれる署名の検証が行われる（ステップ１１１１５）。そして、署名が正しく検証されたか否かにより、消費者１１００が当該署名付きマークの真正性を確認して全ての処理が終了する（ステップ１１１１６）。

【０２３７】上記手順において、消費者１１００による真正性の確認は、たとえば、図１６に示すように表示装置１０２に「本物です」（あるいは「にせものです」、「必要な公開鍵がありません」）といった吹き出しが表示され、消費者１１００が該吹き出しを見ることによって行われる。しかし、別の表示方法を用いてもよい。また、音などを用いて行ってもよいし、音、表示を組み合わせてもよい。

【０２３８】上記の本第５実施形態では、マーク管理者１２０は署名付きマークを受け取る権利がある販売店１１１０にのみ署名付きマークを送付するようにしている。そして、署名付きマークを生成するときの要素として、販売店１１１０のＷｅｂページのＵＲＬデータを用

いている。

【０２３９】また、消費者１１００は、Ｗｅｂページに貼り付けられた署名付きマークの署名を、マーク管理者の公開鍵と該ＷｅｂページのＵＲＬデータとを使って検証するようにしている。

【０２４０】したがって、本第５実施形態によれば、不正者が自己のＷｅｂページに、正規販売者のＷｅｂページからコピーした署名付きマークを貼り付けた場合は、不正者のＷｅｂページのＵＲＬと署名に含まれるＵＲＬとが一致しないため、真正性確認処理で該マークの真正性が確認されない。結果として販売者のＷｅｂページを閲覧する消費者が、そのＷｅｂページに貼り付けられたマークが明示する情報が真正なものであるか否かを正しく確認することができる。

【０２４１】なお、本第５実施形態では、消費者１１００がマークをクリックすることで真正性確認処理が開始されるようにしているが、第４実施形態と同様、Ｗｅｂページを受け取ったときに自動的に真正性確認処理が開始されるようにしてもよい。さらに、該処理において真正性が確認された場合に、当該Ｗｅｂページが表示されるようにしてもよい。

【０２４２】なお、本実施形態における、販売者１１０がマークを取得するステップと消費者１１００が公開鍵を取得するステップとの前後関係は逆でもよい。ただし、本第５実施形態のように、ステップ１１１１０からはじまるＷｅｂページアクセス以前に、消費者１１１００が公開鍵を取得しておけば、Ｗｅｂページアクセスの度に公開鍵を取得する必要がない。

【０２４３】また、本第５実施形態では、販売者端末１１１２とWWWサーバ１１１３とを別マシンとしているが、同一のマシンであってもよい。

【０２４４】さらに、また、本第５実施形態では、ＷｅｂページのＵＲＬデータのみに署名を施すようにしているが、たとえば、マークとして用いている画像データを電子署名の対象に加えてもよい。これにより、販売店１１１０がマーク管理者１１２０より受け取った署名付きマークの署名部分だけを取り出し、自分が加盟店契約していないクレジットカード会社のマークと一纏めにし直すことで、にせの署名付きマークを生成するといった不正を防ぐことができ、より安全性が高まる。さらに、たとえば、販売者１１１０がマークを貼り付けるＷｅｂページをあらかじめ生成し、それをマーク送付要求時にマーク管理者１１２０に送るようにし、該Ｗｅｂページを電子署名の対象に加えてもよい。これにより、別のＷｅｂページに署名付きマークを貼り付けることができなくなり、たとえば、署名付きマークをＷｅｂページの内容証明手段として利用することができるようになる。すなわち、この変形例は、何らかの権威者にＷｅｂページの内容を保証してもらうようなシステムでの利用に適している。

【０２４５】くわえて、本第５実施形態では、署名とマークとを一纏めにして署名付きマークを生成しているが、これは、たとえば、販売者１１０がマークを貼り付けるＷｅｂページをあらかじめ生成し、それをマーク送付要求時にマーク管理者１２０に送るようにし、マーク管理者１２０が該Ｗｅｂページの内容に基づいて作成したフィルタリング用データなどを属性情報として署名付きマークに加えてもよい。

【０２４６】これにより、たとえば、あるＷｅｂページ評価機関が発行した推奨マークが貼られ、かつ、その真正性が正しく確認されたＷｅｂページのみを表示するようフィルタリングすることができる。そのためには、どの種類のマークなら消費者端末１１０１の表示装置１１０２に表示するかということを消費者１１００に設定させるためのフィルタリング設定機能や、それ以外のものなら表示しないようにするようなフィルタリング実行機能などを備えたフィルタリングプログラムを、あらかじめ消費者端末１１０１にインストールしておけばよい。この応用例は、たとえば子どもに見せたくないような暴力表現などを含んだＷｅｂページをフィルタリングしたいようなシステムでの利用に適している。

【０２４７】なお、第４、第５実施形態の各端末、サーバに格納された各プログラムは、一般的には、それぞれの装置を制御するオペレーティングシステムの元で動作し、オペレーティングシステムを介して、装置の各ハードウェア構成要素とデータ、コマンドをやりとりする。もちろん、オペレーティングシステムを介さずに直接、各ハードウェア構成要素とデータ、コマンドをやりとりしても良い。

【０２４８】以上説明したように、第４、第５実施形態によれば、Ｗｅｂページを閲覧するユーザが、そのＷｅｂページに貼り付けられた画像データが明示する情報（ユーザが見た目から判断するであろう情報）が真正なものであるか否かを正しく確認することができる。

【０２４９】以下、本発明の第６の実施形態について説明する。

【０２５０】本第６実施形態の認証システムの構成は、基本的には前記第１実施形態に係る認証システムの構成（図９から図１３参照）と同じである。ただし、消費者端末１１０１のメモリ１２０４中の真正性確認プログラムA１２０４ｃが真正性確認プログラムＣに置き換えられ、マーク管理サーバ１１２２のメモリ１５０７中のマーク管理プログラムA１５０７ｂ が、マーク管理プログラムCに置き換えられら、販売者端末１１２のメモリ１３０６中のマーク取得プログラムが１３０６がマーク取得プログラムcに置き換えられた構成となっている。

【０２５１】以下、本第６実施形態に係る認証システムの動作について説明する。

【０２５２】まず、販売者端末１１１２のマーク取得プログラムcは、自己のＷｅｂページのデータと共にマー

ク送付要求をマーク管理サーバ１１２２に送る。

【０２５３】要求を受けたマーク管理サーバ１１２２の、マーク管理プログラムCは、要求を送った販売者端末１１１２を使用する販売者１１１０に対してマークを送付するか否かを判定し、送付すると判定した場合、図２１に示す処理を行う。

【０２５４】すなわち、マーク管理ＤＢ１１２３に格納しておいたマーク２７０９と、マークに挿入する所定の情報２７０８（たとえば、マーク管理機関１１２１を示すテキストなど）を読み出し、マークに所定の情報を電子透かしとして埋め込む（ステップ２７０５）。そして、電子透かしを埋め込んだマーク２７１０がＷｅｂページ上に表示されるように、マーク送付要求と共に送られたＷｅｂページデータ２７１１を修正し（ステップ２７０６）、修正したＷｅｂページデータ２７１２を販売者端末１１１２のマーク取得プログラムcに送る（ステップ２７０７）。

【０２５５】マーク取得プログラムcは、マーク管理サーバ１１２２から送られたＷｅｂページデータを、WWWサーバ１１１３を介して、webページデータベース１１１４に格納する。

【０２５６】その後、このwebページは、消費者端末１１０１のブラウザプログラム１２０４ｂを介した消費者１１００の要求に応じて消費者端末１１０１に送られ、表示装置１１０２に表示される。

【０２５７】一方、消費者端末１１０１の、真正性確認プログラムCは、消費者１１００からの要求に応じて（たとえばマークのクリックに応じて）、webページの真正性確認処理を行う。

【０２５８】この処理では、図２２に示すように、まず、webページ２９０８から真正性を確認するマーク２９０９を切り出し（ステップ２９０５）、切り出したマーク２９０９に電子透かしとして埋め込まれた情報２９１０を抽出し（ステップ２９０６）、これを表示装置１１０２に表示する（ステップ２９０７）。

【０２５９】ここで、切り出したマーク２９０９から電子透かしとして埋め込まれた情報２９１０９を抽出するために必要な情報（この情報としては、たとえば、図２１の７１０の電子透かしが施される前のオリジナルのマークや、オリジナルのマークとの差分より情報を復元するためのアルゴリズムを特定する情報などが該当する場合がある）は、マーク管理サーバ１１２２から予め入手しておくようにする。このためには、真正性確認プログラムＣ２２０４が消費者１１００の要求に応じてマーク管理サーバ１１２２に真正性確認用情報の要求を送り、その応答として送られた情報をメモリ１２０４や記憶装置１２０２に記憶しておくようにする。また、マーク管理サーバ１１２２の、マーク管理プログラムC２５０７ｂは、真正性確認用情報の要求を受け取った場合には、必要な情報を消費者端末１１０１に送るようにする。

【０２６０】以上、本発明の第６の実施形態について説明した。

【０２６１】本第６実施形態によれば、単なるマークに代えて、電子透かしを施したマークをwebページ上に設けるので、そのマークよりwebページとマークが示す個人／機関との関係の真正性が認証可能となるのみならず、webページによって直接、マークの形態で、そのwebページと関係がある個人／機関を提示することができる。また、webページ上の存在に不自然さのないマークを利用してwebページとマークが示す個人／機関との関係の真正性が認証可能とするので、本第６実施形態によってwebページが不自然な形態に損なわれることはない。

【０２６２】以下、本発明の第７実施形態について説明する。

【０２６３】本第７実施形態の認証システムの構成は、基本的には前記第１実施形態に係る認証システムの構成（図９から図１３参照）と同じである。ただし、消費者端末１１０１のメモリ１２０４中の真正性確認プログラムA１２０４ｃが真正性確認プログラムdに置き換えられ、マーク管理サーバ１１２２のメモリ１５０７中のマーク管理プログラムA１５０７ｂが、マーク管理プログラムdに置き換えられら、販売者端末１１２のメモリ１３０６中のマーク取得プログラムが１３０６がマーク取得プログラムdに置き換えられた構成となっている。

【０２６４】以下、本第７実施形態に係る認証システムの動作について説明する。

【０２６５】まず、販売者端末１１１２のマーク取得プログラムdは、自己のＷｅｂページのデータと共にマーク送付要求をマーク管理サーバ１１２２に送る。

【０２６６】要求を受けたマーク管理サーバ１１２２の、マーク管理プログラムdは、要求を送った販売者端末１１１２を使用する販売者１１１０に対してマークを送付するか否かを判定し、送付すると判定した場合、図23に示す処理を行う。

【０２６７】すなわち、マーク送付要求と共に送られたＷｅｂページデータ２３０５のハッシュ値２３０６を計算し（ステップ２３０１）、マーク管理ＤＢ１１２３に格納しておいたマーク２３０７に、計算したハッシュ値２３０６を電子透かしとして埋め込む（ステップ２３０２）。そして、電子透かしを埋め込んだマーク２３０８がＷｅｂページ上に表示されるように、マーク送付要求と共に送られたＷｅｂページデータ２３０５を修正し（ステップ２３０２）、修正したＷｅｂページデータ２３０９を販売者端末１１１２のマーク取得プログラムdに送る（ステップ２３０４）。

【０２６８】マーク取得プログラムdは、マーク管理サーバ１１２２から送られたＷｅｂページデータを、WWWサーバ１１１３を介して、webページデータベース１１１４に格納する。

【０２６９】その後、このwebページは、消費者端末１１０１のブラウザプログラム１２０４ｂを介した消費者１１００の要求に応じて消費者端末１１０１に送られ、表示装置１１０２に表示される。

【０２７０】一方、消費者端末１１０１の、真正性確認プログラムｄは、消費者１１００からの要求に応じて（たとえばマークのクリックに応じて）、webページの真正性確認処理を行う。

【０２７１】この処理では、図２４に示すように、まず、webページ２４０６から真正性を確認するマーク２４０７を切り出し（ステップ２４０１）、切り出したマーク２４０７に電子透かしとして埋め込まれたハッシュ値２４０８を抽出する（ステップ２４０２）。また、webページ２４０６から真正性を確認するマークに関連する部分を除いたwebページデータのハッシュ値２４０９を計算し（ステップ２４０９）、これとマークから抽出したハッシュ値２４０８とを比較する（ステップ２４０４）。そして、一致した場合には、真正性が確認できたことを、一致しない場合には、真正性が確認できなかったことを表示装置１１０２に表示する（ステップ２４０５）。

【０２７２】なお、切り出したマークから電子透かしとして埋め込まれたハッシュ値を抽出するために必要な情報は、マーク管理サーバ１１２２から予め入手しておくようにする。このためには、真正性確認プログラムｄが消費者１１００の要求に応じてマーク管理サーバ１１２２に真正性確認用情報の要求を送り、その応答として送られた情報をメモリ１２０４や記憶装置１２０２に記憶しておくようにする。また、マーク管理サーバ１１２２の、マーク管理プログラムｄは、真正性確認用情報の要求を受け取った場合には、必要な情報を消費者端末１１０１に送るようにする。

【０２７３】本第７実施形態によれば、単なるマークに代えて、webページのハッシュ値を電子透かしとして施したマークをwebページ上に設けるので、そのマークより当該マークが確かに、そのマークを含むwebページに対して与えられたものであることが認証可能となるのみならず、webページによって直接、マークの形態で、そのwebページと関係がある個人／機関を提示することができる。また、電子透かしとしてwebページデータのハッシュ値を用い、これを特定の種類のデータであるマークの電子透かしとして用いるので、webページが複数種のデータを含んでいるかどうかに依存することなく、同一の処理で処理を行うことができる。また、webページ上の存在に不自然さのないマークを利用して、webページに対して真にマークが与えられたことを認証可能とするので、本第７実施形態によってwebページが不自然な形態に損なわれることはない。

【０２７４】以下、本発明の第８の実施形態について説明する。

【０２７５】本第８実施形態に係る認証システムは、基本的には前記第１実施形態に係る認証システムの構成（図９から図１３参照）と同じである。

【０２７６】ただし、消費者端末１１０１については、図２５に示すように、前記第５実施形態で説明した公開鍵ＤＢ１８０１が接続されている点と、公開鍵ＤＢインタフェース１９００を備えている点と、メモリ１２０４中の真正性確認プログラムA１２０４ｃが真正性確認プログラムe３２０４に置き換えられている点が異なる。

【０２７７】また、マーク管理サーバ１１２２については、図２６に示すように、メモリ１５０７中のマーク管理プログラムA１５０７ｂが、マーク管理プログラムe３５０７に置き換えられらている点が異なる。

【０２７８】また、図２７に示すように、販売者端末１１２については、メモリ１３０６中のマーク取得プログラムが１３０６がマーク取得プログラムe3306に置き換えられた構成となっている点が異なる。

【０２７９】以下、本第８実施形態に係る認証システムの動作について説明する。

【０２８０】まず、販売者端末１１１２のマーク取得プログラムdは、自己のＷｅｂページのデータと共にマーク送付要求をマーク管理サーバ１１２２に送る。

【０２８１】要求を受けたマーク管理サーバ１１２２の、マーク管理プログラムdは、要求を送った販売者端末１１１２を使用する販売者１１１０に対してマークを送付するか否かを判定し、送付すると判定した場合、図２８に示す処理を行う。

【０２８２】すなわち、マーク送付要求と共に送られたＷｅｂページデータ２８０６のハッシュ値２８０７を計算し（ステップ２８０１）、ハッシュ値２８０７をマーク管理機関の秘密鍵２８０８で暗号化した電子署名２８０９を作成し（ステップ２８０２）、これをマーク管理ＤＢ１１２３に格納しておいたマーク２８１０に、電子透かしとして埋め込む（ステップ２８０３）。そして、電子透かしを埋め込んだマーク２８１１がＷｅｂページ上に表示されるように、マーク送付要求と共に送られたＷｅｂページデータ２８０６を修正し（ステップ２８０４）、修正したＷｅｂページデータ２８１２を販売者端末１１１２のマーク取得プログラムeに送る（ステップ２８０５）。

【０２８３】マーク取得プログラムeは、マーク管理サーバ１１２２から送られたＷｅｂページデータを、WWWサーバ１１１３を介して、webページデータベース１１１４に格納する。

【０２８４】その後、このwebページは、消費者端末１１０１のブラウザプログラム１２０４ｂを介した消費者１１００の要求に応じて消費者端末１１０１に送られ、表示装置１１０２に表示される。

【０２８５】一方、消費者端末１１０１の、真正性確認プログラムｄは、消費者１１００からの要求に応じて

（たとえばマークのクリックに応じて）、webページの真正性確認処理を行う。

【０２８６】この処理では、図２９に示すように、まず、公開鍵ＤＢ１８０１からマーク管理機関の公開鍵２９０８を取り出す。そして、webページ２９０７から真正性を確認するマーク２９０８を切り出し（ステップ２９０１）、切り出したマーク２９０８に電子透かしとして埋め込まれた電子署名２９０９を抽出し（ステップ２９０２）、マーク管理機関の公開鍵２９１０により復号化してハッシュ値を抽出する（ステップ２９０３）。また、webページ２９０７から真正性を確認するマークに関連する部分を除いたwebページデータのハッシュ値２９１２を計算し（ステップ２９０４）、これとマークから抽出した電子署名を復号化したハッシュ値２９１１とを比較する（ステップ２９０５）。そして、一致した場合には、真正性が確認できたことを、一致しない場合には、真正性が確認できなかったことを表示装置１１０２に表示する（ステップ２９０６）。

【０２８７】なお、切り出したマークから電子透かしとして埋め込まれたハッシュ値を抽出するために必要な情報は、マーク管理サーバ１１２２から予め入手しておくようにする。このためには、真正性確認プログラムeが消費者１１００の要求に応じてマーク管理サーバ１１２２に真正性確認用情報の要求を送り、その応答として送られた情報をメモリ１２０４や記憶装置１２０２に記憶しておくようにする。また、マーク管理サーバ１１２２の、マーク管理プログラムeは、真正性確認用情報の要求を受け取った場合には、必要な情報を消費者端末１１０１に送るようにする。

【０２８８】また、マーク管理機関の公開鍵は、消費者端末１１００より、公開鍵送付要求をマーク管理サーバ１１１３に送り、その応答として受けとった公開鍵を公開鍵ＤＢ１８０１に格納するようにする。また、公開鍵送付要求を受け取ったマーク管理サーバ１１１３は、自己の公開鍵を応答として消費者端末１１００に返送するようにする。

【０２８９】以上のように、本第８実施形態によれば、単なるマークに代えて、webページのハッシュ値をマーク管理機関の秘密鍵で暗号化した電子署名を電子透かしとして施したマークをwebページ上に設けるので、そのマークより当該マークが確かに、そのマークを含むwebページに対して、マーク管理機関によって与えられたものであることが認証可能となるのみならず、webページによって直接、マークの形態で、そのwebページと関係がある個人／機関を提示することができる。また、webページデータのハッシュ値を対象とした電子署名を、これを特定の種類のデータであるマークの電子透かしとして用いるので、webページが複数種のデータを含んでいるかどうかに依存することなく、同一の処理で処理を行うことができる。また、電子署名を電子透かしとしてwebページ上のマークに埋め込むので、webページデータと別個に電子署名を管理する必要はない。また、存在に不自然さのないマークを利用して、webページと個人／機関の関係を認証可能とするので、本第８実施形態によってwebページが不自然な形態に損なわれることはない。

【０２９０】なお、以上の第６実施形態から第８実施形態では、マーク管理サーバ１１２２において、電子透かしを埋め込んだマークがＷｅｂページ上に表示されるように、マーク送付要求と共に送られたＷｅｂページデータを修正し（ステップ２８０４）、修正したＷｅｂページデータ２８１２を販売者端末１１１２のマーク取得プログラムeに送る処理を行ったが、これは、次のように修正するようにしてもよい。

【０２９１】すなわち、マーク管理サーバ１１２２において、電子透かしを埋め込んだマークを販売者端末１１１２に送る。そして、販売者端末１１１２において、電子透かしを埋め込んだマークがＷｅｂページ上に表示されるように、マーク送付要求と共に送くったＷｅｂページデータのオリジナルを修正する。

【０２９２】また、以上の第６実施形態から第８実施形態では、消費者端末１１０１における処理に変えて次の処理を行うようにしてもよい。

【０２９３】すなわち、第６実施形態の場合は、消費者端末１１０１は、webページから真正性を確認するマークを切り出し、切り出したマークと共にマーク管理サーバ１１２２に真正性確認を要求する。また、第７、第８実施形態の場合は、マークを含むwebページのデータと共にマーク管理サーバ１１２２に真正性確認を要求する。そして、この要求の応答として、マーク管理サーバ１１２２から送られた、真正性が確認できた、もしくは、真正性が確認できなかった旨のメッセージを表示装置１１０２に表示する。一方、マーク管理サーバ１１２２は、真正性確認を要求されたならば、その要求と共に送られたマークについて、第６実施形態から第８実施形態で消費者端末１１０１において行っていた処理を行う。すなわち、、第６実施形態の場合は、要求と共に送られたマークに電子透かしとして埋め込まれた情報を抽出し、これがマーク管理サーバ１１２２において埋め込んだ情報と一致していれば、真正性が確認できた旨のメッセージを消費者端末１１０１に送り、一致してなければ真正性が確認できなかった旨のメッセージを消費者端末１１０１に送る。また、第７実施形態の場合は、要求と共に送られたwebページからマークを切り出し、切り出したマークに電子透かしとして埋め込まれたハッシュ値を抽出し、要求と共に送られたwebページから真正性を確認するマークに関連する部分を除いたwebページデータのハッシュ値を計算し、これとマークから抽出したハッシュ値２４０８とを比較する。そして、一致した場合には、真正性が確認できた旨のメッセージを消費者端末１１０１に送り、一致してなければ真正性が確認でき

なかった旨のメッセージを消費者端末１１０１に送る。また第８実施形態の場合は、、要求と共に送られたwebページからマークを切り出し、切り出したマークに電子透かしとして埋め込まれた電子署名を抽出し、マーク管理機関の公開鍵により復号化してハッシュ値を抽出する。また、要求と共に送られたwebページから真正性を確認するマークに関連する部分を除いたwebページデータのハッシュ値を計算し、これとマークから抽出した電子署名を復号化したハッシュ値とを比較する。そして、一致した場合には、真正性が確認できた旨のメッセージを消費者端末１１０１に送り、一致してなければ真正性が確認できなかった旨のメッセージを消費者端末１１０１に送る。

【０２９４】ところで、以上の第６実施形態から第８実施形態は、webページの他、 各種電子商取引の対象となる電子データについて適用可能である。たとえば、各種電子商取引の対象が、図面を表すドロウデータである場合に、当該図面に販売者のマークを付けて、当該図面が真正なものであることを認証可能とするような用途に使用することができる。また、前述したように、マークは必ずしもイメージデータでなくてもよい。たとえば、各種電子商取引の対象がオウディオデータである場合に、オウディオデータの前後に販売者や著作権者を示すオウディオデータをマークとして付加し、この付加したマークに第６実施形態から第８実施形態で埋め込んだ電子透かしを埋め込むようにしてもよい。

【０２９５】以上、本発明の各実施形態について説明した。

【０２９６】なお、以上の各実施形態におけるプログラムは、フロッピーディスク、ＣＤ－ＲＯＭ、ＤＶＤ等各種記憶媒体に格納された形態で、プログラムを事項する各装置に供給するか、あるいはこれらの装置が接続されたネットワークに接続された他のサーバから当該装置にダウンロードするようにしてもよい。

【０２９７】また、以上の各実施形態は、その要旨を逸脱しない範囲内で、さまざまに修正することができる。

【０２９８】

【発明の効果】以上のように、本発明によれば、電子データと個人／機関との関係を、より高い信頼性をもって認証可能とする技術を提供することができる。また、電子データとの関係を認証可能な個人／機関と一致することが保証されるように、電子データと関係を持つ個人／機関を電子データによって利用者に直接提示ことができる。

【図面の簡単な説明】

【図１】本発明の第１実施形態に係るコンテンツ配布システムの構成を示すブロック図である。

【図２】本発明の第１実施形態に係るプロバイダー装置と購入者装置の構成を示すブロック図である。

【図３】本発明の第１実施形態に係る電子計算機の一般的な構成を示したブロック図である。

【図４】本発明の第１実施形態に係るコンテンツ配布の処理手順を示したフローチャートである。

【図５】本発明の第１実施形態に係るコンテンツ配布の処理手順を示したフローチャートである。

【図６】本発明の第１実施形態に係るコンテンツ配布の処理手順を示したフローチャートである。

【図７】本発明の第２実施形態に係る第２配布コンテンツ作成システムの構成を示すブロック図である。

【図８】本発明の第２実施形態に係るプロバイダー装置と権利者装置の構成を示すブロック図である。

【図９】本発明の第４実施形態に係る認証システムの概略構成を示すブロック図である。

【図１０】本発明の第４実施形態に係る消費者端末のハードウェア構成を示すブロック図である。

【図１１】本発明の第４実施形態に係る販売者端末のハードウェア構成を示すブロック図である。

【図１２】本発明の第４実施形態に係るＷＷＷサーバのハードウェア構成を示すブロック図である。

【図１３】本発明の第４実施形態に係る管理サーバのハードウェア構成を示すブロック図である。

【図１４】本発明の第４実施形態に係る認証システムの動作を示すフローチャートである。

【図１５】本発明の第４実施形態に係るマーク管理ＤＢの内容を示す図である。

【図１６】本発明の第５実施形態に係る認証システムの概略構成を示すブロック図である。

【図１７】本発明の第５実施形態に係る消費者端末のハードウェア構成を示すブロック図である。

【図１８】本発明の第５実施形態に係るマーク管理サーバのハードウェア構成を示すブロック図である。

【図１９】本発明の第５実施形態に係る認証システムの動作を示すフローチャートである。

【図２０】本発明の第５実施形態に係るマーク管理ＤＢの内容を示す図である。

【図２１】本発明の第６実施形態に係るマーク管理サーバの動作を示すフローチャートである。

【図２２】本発明の第６実施形態に係る消費者端末の動作を示すフローチャートである。

【図２３】本発明の第７実施形態に係るマーク管理サーバの動作を示すフローチャートである。

【図２４】本発明の第７実施形態に係る消費者端末の動作を示すフローチャートである。

【図２５】本発明の第８実施形態に係る消費者端末のハードウェア構成を示すブロック図である。

【図２６】本発明の第８実施形態に係るマーク管理サーバのハードウェア構成を示すブロック図である。

【図２７】本発明の第８実施形態に係る販売者端末のハードウェア構成を示すブロック図である。

【図２８】本発明の第８実施形態に係るマーク管理サー

バの動作を示すフローチャートである。

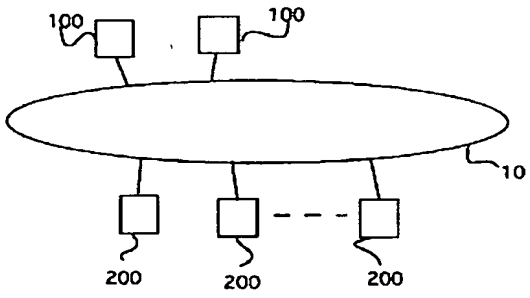
【図２９】本発明の第８実施形態に係る消費者端末の動作を示すフローチャートである。

【符号の説明】

１０　ネットワーク
１００　プロバイダー装置
１１０　処理部
１１１　入出力部
１１２　制御部
１１３　署名抽出部
１１４　署名検証部
１１５　暗号化部
１１６　送受信部
１２０　記憶部
２００　購入者装置
２１０、７１０　処理部
２１１、７１１　入出力部
２１２、７１２　制御部
２１３、７１３　送受信部
２１４、７１４　復号化部
２１５、７１５　署名生成部
２１６、７１５　署名埋め込み部
２１７、７１７　鍵生成部
２２０、７２０　記憶部
１１００（１０００-１～１０００-ｎ）：消費者、
１１０１（１１０１-１～１１０１-ｎ）、１８００（１８００-１～１８００-ｎ）：消費者端末、
１１０２、１３０１、１４０１、１５０１：表示装置、
１１０３（１１０３-１～１１０３-２）、１３０２、１４０２、１５０２：入力装置、
１１１０：販売者、
１１１１：販売店、
１１１２：販売者端末、
１１１３：ＷＷＷサーバ、
１１１４：ＷｅｂページＤＢ、
１１２０：マーク管理者、
１１２１：マーク管理機関、
１１２２、１８１０：マーク管理サーバ、
１１２３：マーク管理ＤＢ、
１１４０：通信網、
１２００、１３００、１４００、１５００：バス、
１２０１、１３０３、１４０３、１５０３：通信網インタフェース、
１２０２、１３０４、１４０５、１５０５：記憶装置、
１２０３、１３０５、１４０６、１５０６：ＣＰＵ、
１２０４、１３０６、１４０７、１５０７、１９０１、１１０００：メモリ、

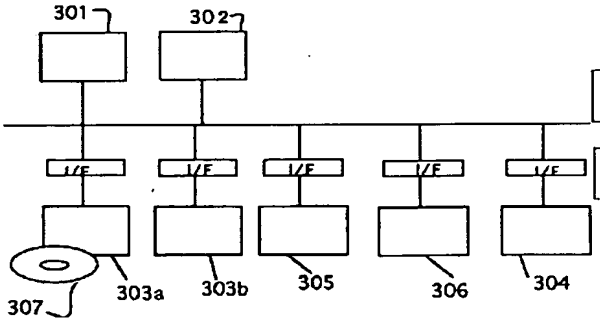
【図１】

図１



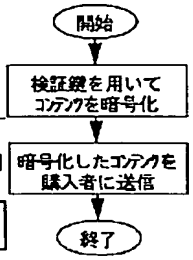
【図３】

図３



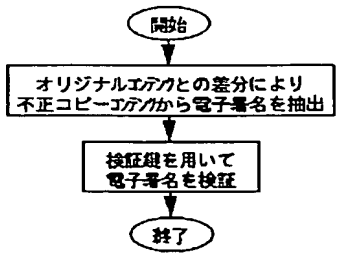
【図４】

図４



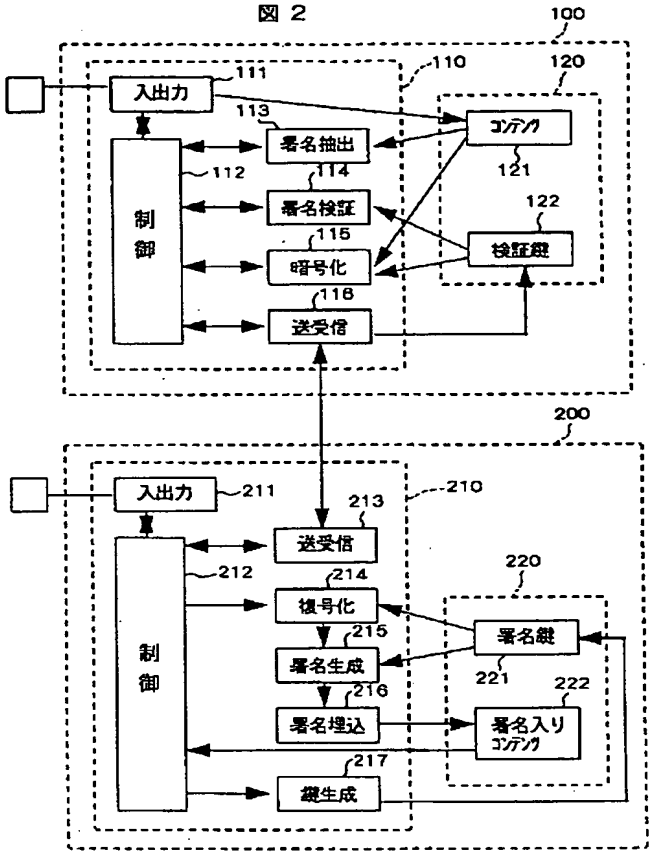
【図６】

図６



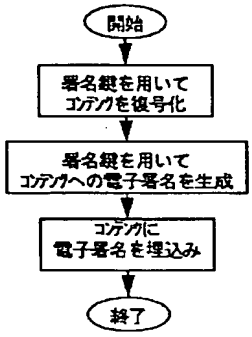
【図２】

図 2



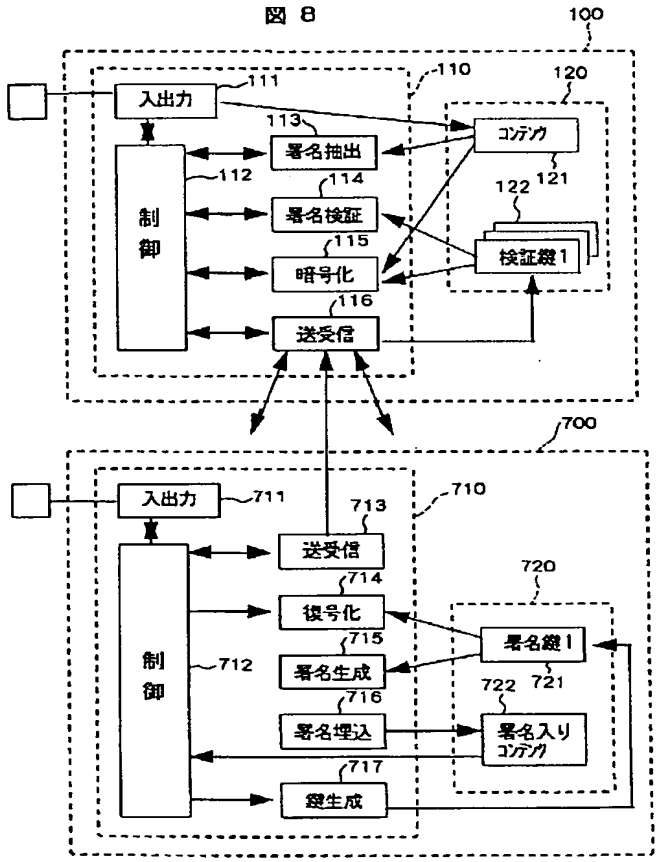
【図５】

図 5



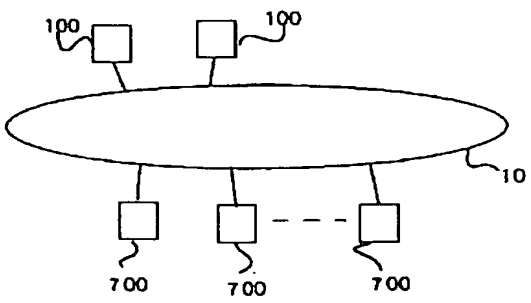
【図８】

図 8



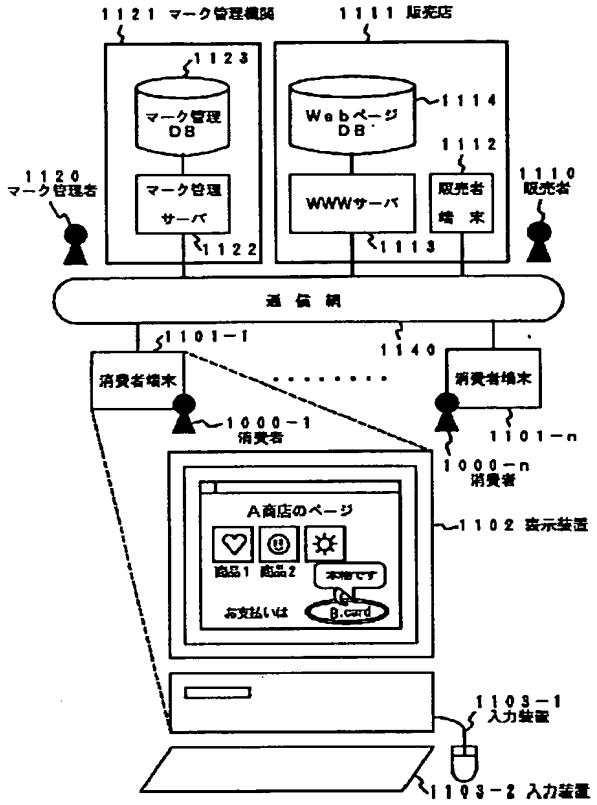
【図７】

図 7



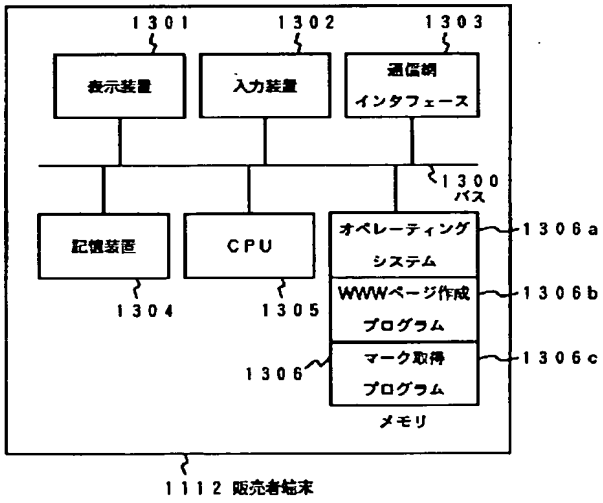
【図９】

図 9



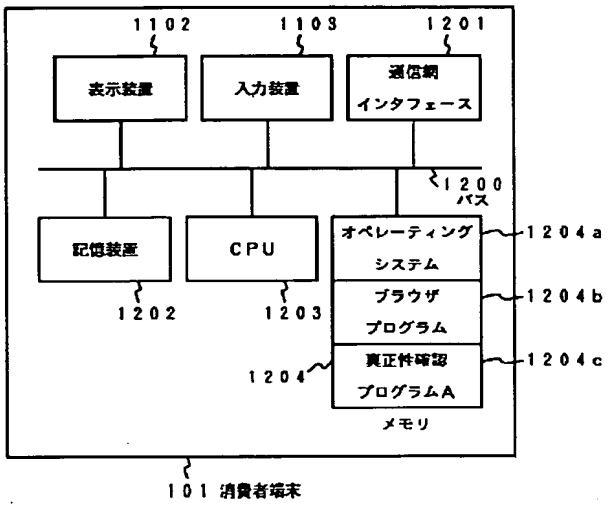
【図１１】

図11



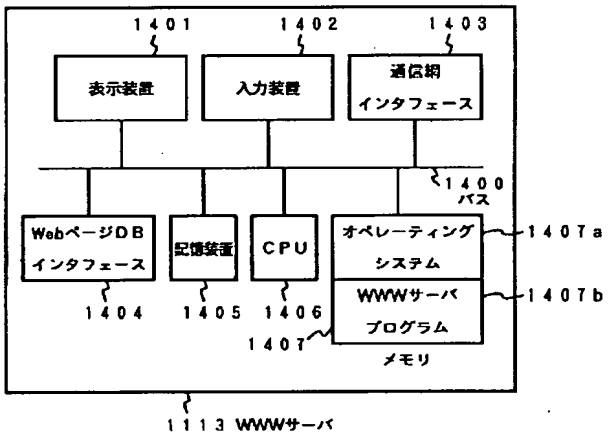
【図１０】

図10



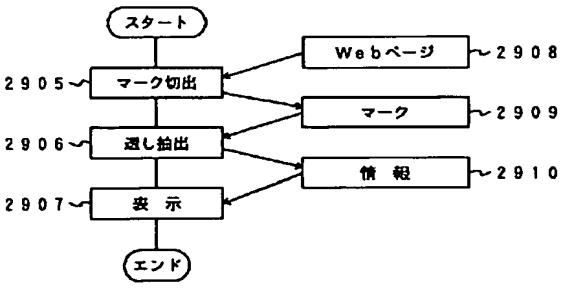
【図１２】

図12



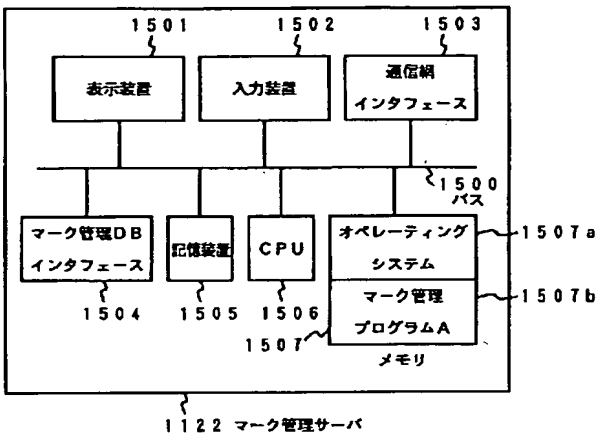
【図２２】

図22



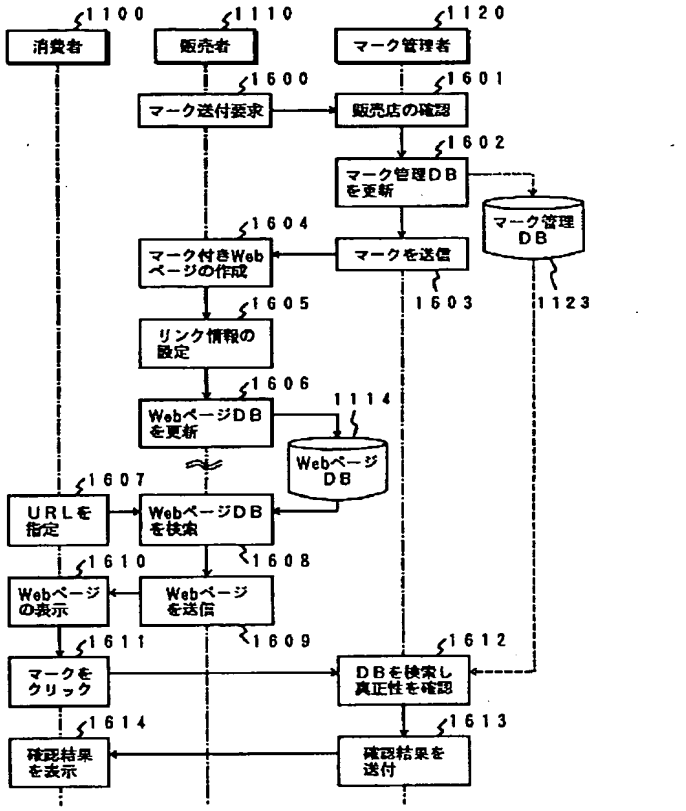
【図１３】

図13



【図１４】

図14



【図１５】

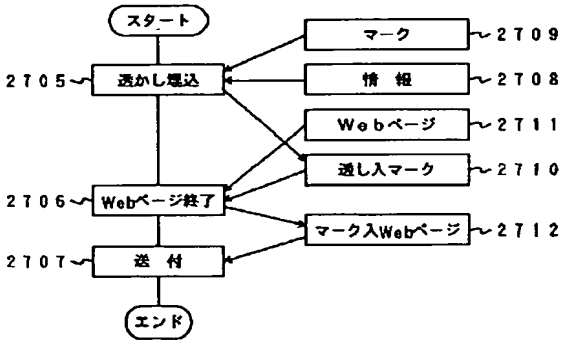
図15

No	日　時（有効期限）	マーク種別	販売者	販売店のＵＲＬ
1	1998. 1. 1～1999. 12. 31	B. Card	A	www. a. co. jp
2	1998. 1. 1～1999. 12. 31	B. Card	C	www. c. co. jp
3	1998. 4. 1～2001. 3. 31	Card. E	A	www. a. co. jp
4	1997. 5. 1～1998. 4. 30	B. Card	D	www. d. co. jp
:	:	:	:	:

1123 マーク管理ＤＢ

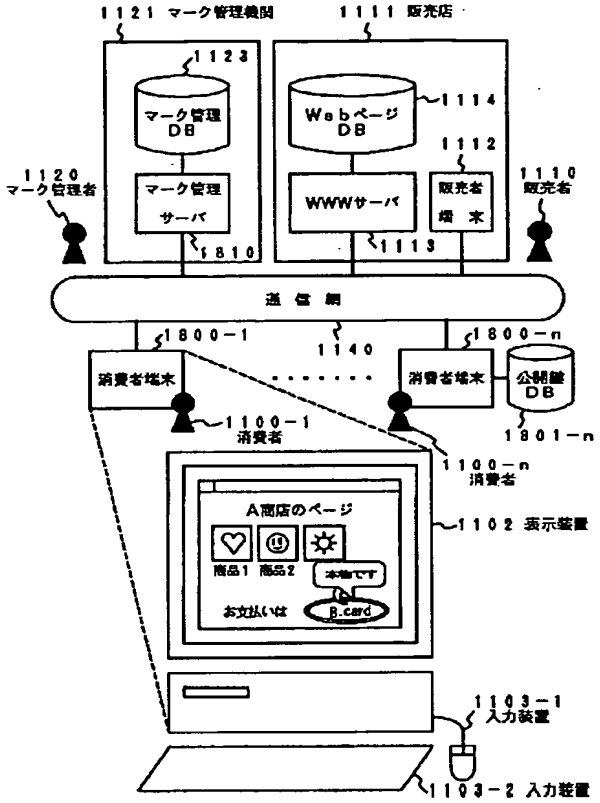
【図２１】

図21



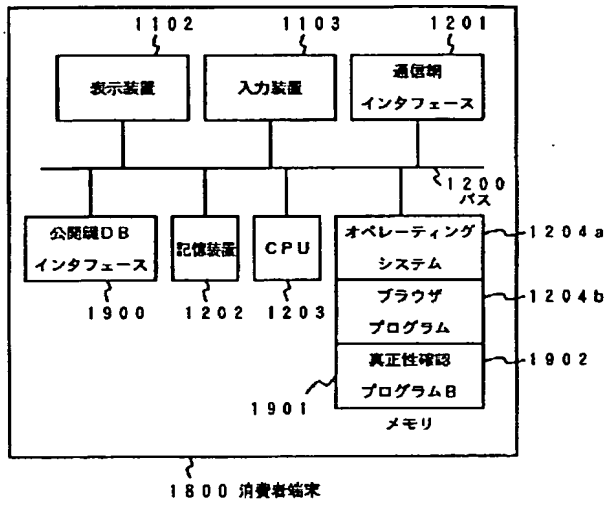
【図１６】

図16



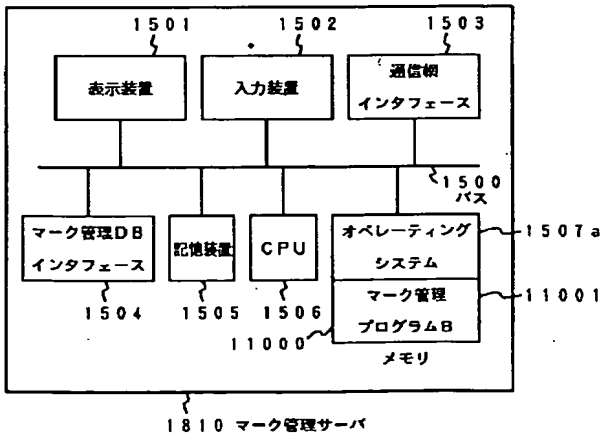
【図１７】

図17



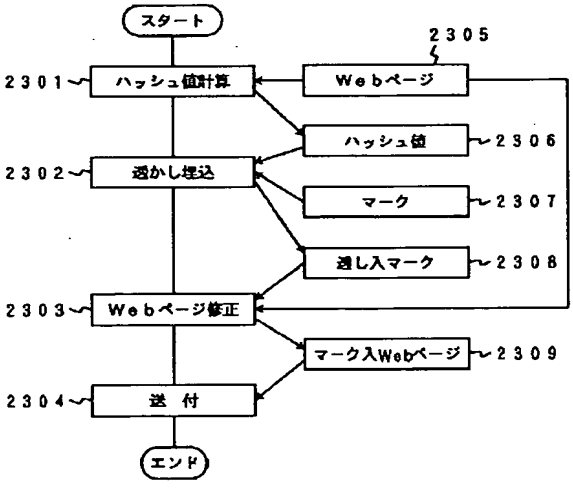
【図１８】

図18



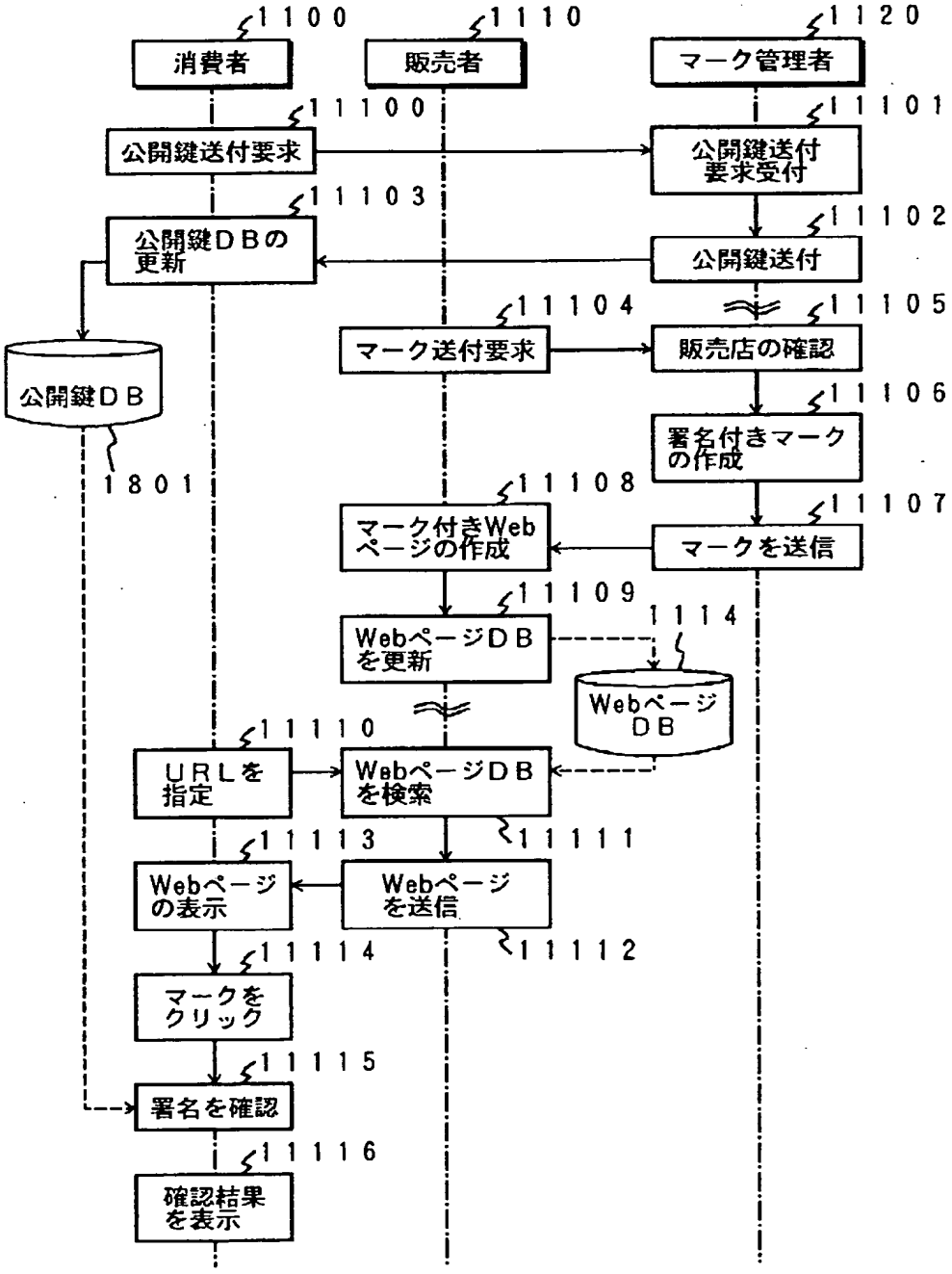
【図２３】

図23



【図１９】

図19


1100
消費者
1110
販売者
1120
マーク管理者
11100
公開鍵送付要求
11101
公開鍵送付要求受付
11103
公開鍵ＤＢの更新
11102
公開鍵送付
11104
マーク送付要求
11105
販売店の確認
公開鍵ＤＢ
1801
11106
署名付きマークの作成
11108
マーク付きWebページの作成
11107
マークを送信
11109
WebページＤＢを更新
1114
Webページ ＤＢ
11110
ＵＲＬを指定
WebページＤＢを検索
11113
11111
Webページの表示
Webページを送信
11112
11114
マークをクリック
11115
署名を確認
11116
確認結果を表示

【図２０】

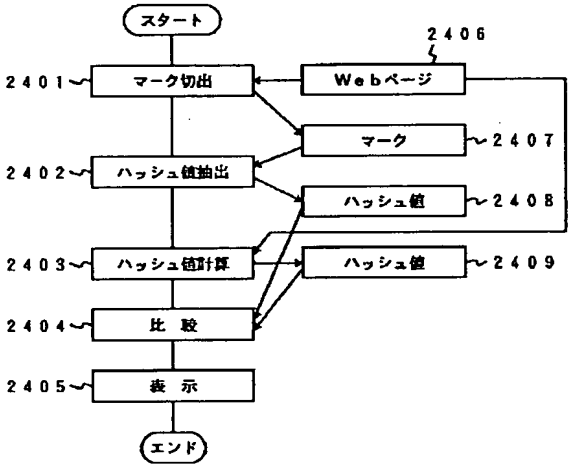
図２０

No	マーク管理者	有効期間	公　開　鍵
1	α	1997. 1. 1～1998. 12. 31	dayh8u4uf75kwef85o3yd
2	β	1997. 1. 1～1998. 12. 31	gfijvklsjt867wrf586d84w
3	γ	1997. 4. 1～1999. 3. 31	u57di853riwdyp0695utc7
4	δ	1997. 1. 1～1998. 12. 31	ysfyw65uscm3140abyds
:	:	:	:

１８０１ 公開鍵ＤＢ

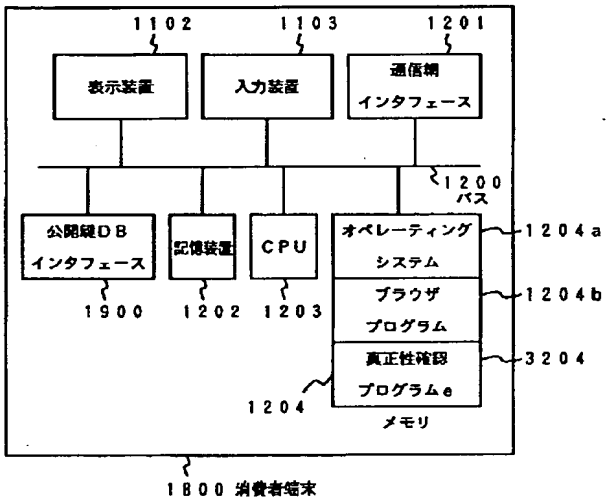
【図２４】

図２４



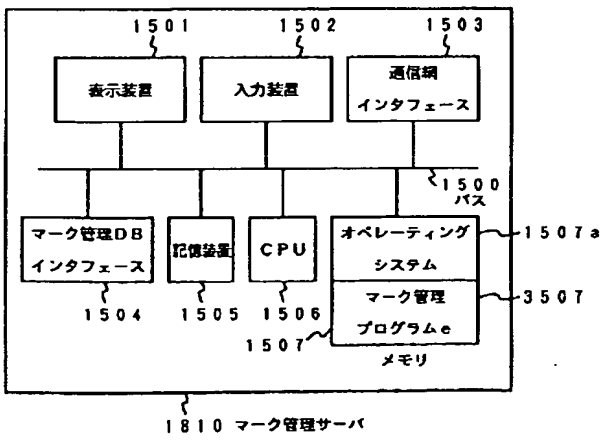
【図２５】

図２５



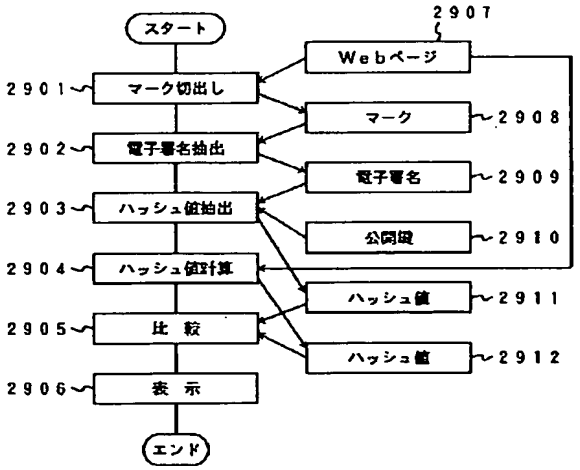
【図２６】

図２６



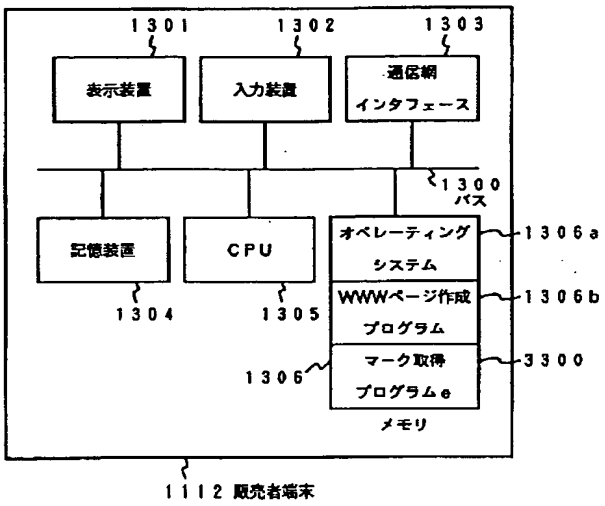
【図２９】

図２９



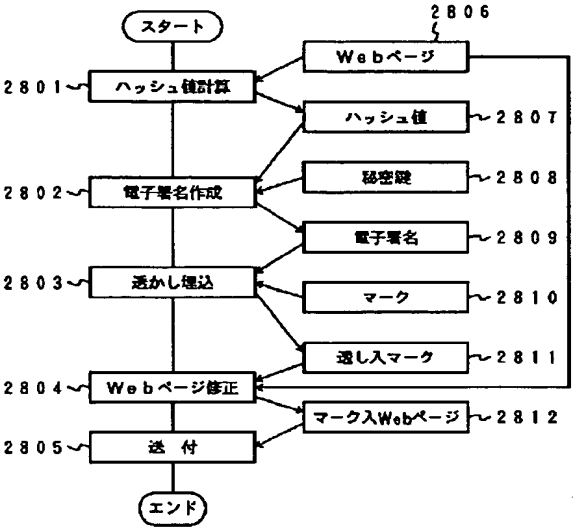
【図２７】

図27



【図２８】

図28



フロントページの続き

(51)Int.Cl.[6]　　識別記号
H０４N　1/387

F I
H０４N　1/387

(72)発明者　佐々木　良一
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　豊島　久
東京都江島区新砂一丁目６番27号　株式会社日立製作所公共情報事業部内

(72)発明者　齋藤　司
東京都江島区新砂一丁目６番27号　株式会社日立製作所公共情報事業部内